Financial crime and fraud

Khashayar Naimi

Content

Financial crime

Financial crime is crime committed against property, involving the unlawful conversion of the ownership of property (belonging to one person) to one's own personal use and benefit. Financial crimes may involve fraud (cheque fraud, credit card fraud, mortgage fraud, medical fraud, corporate fraud, securities fraud (including insider trading), bank fraud, insurance fraud, market manipulation, payment (point of sale) fraud, health care fraud); theft; scams or confidence tricks; tax evasion; bribery; embezzlement; identity theft; money laundering; and forgery and counterfeiting, including the production of Counterfeit money and consumer goods.

Financial crimes may involve additional criminal acts, such as computer crime, elder abuse, burglary, armed robbery, and even violent crime such as robbery or murder. Financial crimes may be carried out by individuals, corporations, or by organized crime groups. Victims may include individuals, corporations, governments, and entire economies.

The U.S. introduced the Foreign Corrupt Practices Act in 1977 to address bribery of foreign officials. This legislation dominated international anti-corruption enforcement until around 2010 when other countries began introducing broader and more robust legislation, notably the United Kingdom Bribery Act 2010. The International Organization for Standardization introduced an international anti-bribery management system standard in 2016. In recent years, cooperation in enforcement action between countries has increased.

For most countries, money laundering and terrorist financing raise significant issues with regard to prevention, detection and prosecution. Sophisticated techniques used to launder money and finance terrorism add to the complexity of these issues. Such sophisticated techniques may involve different types of financial institutions; multiple financial transactions; the use of intermediaries, such as financial advisers, accountants, shell corporations and other service providers; transfers to, through, and from different countries; and the use of different financial instruments and other kinds of value-storing assets. Money laundering is, however, a fundamentally simple concept. It is the process by which proceeds from a criminal activity are disguised to conceal their true origin. Basically, money laundering involves the proceeds of criminally derived property rather than the property itself. Money laundering can be defined in a number of ways, most countries subscribe to the definition adopted by the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (Vienna Convention) and the United Nations Convention Against Transnational Organized Crime (2000) (Palermo Convention):

i. The conversion or transfer of property, knowing that such property is derived from any (drug trafficking) offense or offenses or from an act of participation in such offense or offenses, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offense or offenses to evade the legal consequences of his actions;

ii. The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offense or offenses or from an act of participation in such an offense or offenses, and;

iii. The acquisition, possession or use of property, knowing at the time of receipt that such property was derived from an offense or offenses or from an act of Participation in such offense or offenses.

The Financial Action Task Force on Money Laundering (FATF), which is recognized as the international standard setter for Anti-money Laundering (AML) efforts, defines the term "money laundering" briefly as "the processing of criminal proceeds to disguise their illegal origin" in order to "legitimize" the ill-gotten gains of crime.

In 2005, money laundering within the financial industry in the UK was believed to amount to £25bn a year.

In 2005, fraud within the financial industry was estimated to cost the UK £14bn a year.

Bank fraud

Bank fraud is the use of potentially illegal means to obtain money, assets, or other property owned or held by a financial institution, or to obtain money from depositors by fraudulently posing as a bank or other financial institution. In many instances, bank fraud is a criminal offence. While the specific elements of particular banking fraud laws vary depending on jurisdictions, the term bank fraud applies to actions that employ a scheme or artifice, as opposed to bank robbery or theft. For this reason, bank fraud is sometimes considered a white-collar crime.

Fraudsters may seek access to facilities such as mailrooms, post offices, offices of a tax authority, a corporate payroll or a social or veterans' benefit office, which process cheques in large numbers. The fraudsters then may open bank accounts under assumed names and deposit the cheques, which they may first alter in order to appear legitimate, so that they can subsequently withdraw unauthorised funds.

Alternatively, forgers gain unauthorised access to blank chequebooks, and forge seemingly legitimate signatures on the cheques, also in order to illegally gain access to unauthorized funds.

Cheque kiting exploits a banking system known as "the float" wherein money is temporarily counted twice. When a cheque is deposited to an account at Bank X, the money is made available immediately in that account even though the corresponding amount of money is not immediately removed from the account at Bank Y at which the cheque is drawn. Thus both banks temporarily count the cheque amount as an asset until the cheque formally clears at Bank Y. The float serves a legitimate purpose in banking, but intentionally exploiting the float when funds at Bank Y are insufficient to cover the amount withdrawn from Bank X is a form of fraud.

Fraudsters have altered cheques to change the name (in order to deposit cheques intended for payment to someone else) or the amount on the face of cheques, simple altering can change $100.00 into $100,000.00. (However, transactions for such large values are routinely investigated as a matter of policy to prevent fraud.)

Instead of tampering with a real cheque, fraudsters may alternatively attempt to forge a depositor's signature on a blank cheque or even print their own cheques drawn on accounts owned by others, non-existent accounts, etc. They would subsequently cash the fraudulent cheque through another bank and withdraw the money before the banks realise that the cheque was a fraud.

In order to hide serious financial problems, some businesses have been known to use fraudulent bookkeeping to overstate sales and income, inflate the worth of the company's assets, or state a profit when the company is operating at a loss. These tampered records are then used to seek investment in the company's bond or security issues or to make fraudulent loan applications in a final attempt to obtain more money to delay the inevitable collapse of an unprofitable or mismanaged firm. Examples of accounting frauds: Enron and WorldCom and Ocala Funding. These companies "cooked the books" in order to appear as though they had profits each quarter, when in fact they were deeply in debt.

A bank soliciting public deposits may be uninsured or not licensed to operate at all. The objective is usually to solicit for deposits to this uninsured "bank", although some may also sell stock representing ownership of the "bank". Sometimes the names appear very official or very similar to those of legitimate banks. For instance, the unlicensed "Chase Trust Bank" of Washington D.C. appeared in 2002, bearing no affiliation to its seemingly apparent namesake; the real Chase Manhattan Bank is based in New York. Accounting fraud has also been used to conceal other theft taking place within a company.

Demand draft (DD) fraud typically involves one or more corrupt bank employees. Firstly, such employees remove a few DD leaves or DD books from stock and write them like a regular DD. Since they are insiders, they know the coding and punching of a demand draft. Such fraudulent demand drafts are usually drawn payable at a distant city without debiting an account. The draft is cashed at the payable branch. The fraud is discovered only when the bank's head office does the branch-wise reconciliation, which normally take six months, by which time the money is gone.

Remotely created checks are orders of payment created by the payee and authorized by the customer remotely, using a telephone or the internet by providing the required information including the MICR code from a valid check. They do not bear the signatures of the customers like ordinary cheques. Instead, they bear a legend statement "Authorized by Drawer". This type of instrument is usually used by credit card companies, utility companies, or telemarketers. The lack of signature makes them susceptible to fraud. The fraud is considered DD fraud in the US.

A rogue trader is a trader at a financial institution who engages in unauthorized trading to recoup the loss he incurred in earlier trades. Out of fear and desperation, he manipulates the internal controls to circumvent detection to buy more time.

Unfortunately, unauthorized trading activities invariably produce more losses due to time constraints; most rogue traders are discovered at an early stage with losses ranging from $1 million to $100 million, but a very few working out of institutions with extremely lax controls were not discovered until the loss had reached well over a billion dollars. The size of the loss is a reflection of the laxity in controls instituted at the firm and not the trader's greed. Contrary to the public perception, rogue traders do not have criminal intent to defraud his employer to enrich himself; he is merely trying to recoup the loss to make his firm whole and salvage his employment.

One way to remove money from a bank is to take out a loan, which bankers are more than willing to encourage if they have good reason to believe that the money will be repaid in full with interest. A fraudulent loan, however, is one in which the borrower is a business entity controlled by a dishonest bank officer or an accomplice; the "borrower" then declares bankruptcy or vanishes and the money is gone. The borrower may even be a non-existent entity and the loan merely an artifice to conceal a theft of a large sum of money from the bank. This can also seen as a component within mortgage fraud (Bell, 2010).

These take a number of forms varying from individuals using false information to hide a credit history filled with financial problems and unpaid loans to corporations using accounting fraud to overstate profits in order to make a risky loan appear to be a sound investment for the bank.

Forged documents are often used to conceal other thefts; banks tend to count their money meticulously so every penny must be accounted for. A document claiming that a sum of money has been borrowed as a loan, withdrawn by an individual depositor or transferred or invested can therefore be valuable to someone who wishes to conceal the minor detail that the bank's money has in fact been stolen and is now gone.

Wire transfer networks such as the international SWIFT interbank fund transfer system are tempting as targets as a transfer, once made, is difficult or impossible to reverse. As these networks are used by banks to settle accounts with each other, rapid or overnight wire transfer of large amounts of money are commonplace; while banks have put checks and balances in place, there is the risk that insiders may attempt to use fraudulent or forged documents which claim to request a bank depositor's money be wired to another bank, often an offshore account in some distant foreign country.

There is a very high risk of fraud when dealing with unknown or uninsured institutions.

The risk is greatest when dealing with offshore or Internet banks (as this allows selection of countries with lax banking regulations), but not by any means limited to these institutions. There is an annual list of unlicensed banks on the US Treasury Department web site which currently is fifteen pages in length.

Also, a person may send a wire transfer from country to country. Since this takes a few days for the transfer to "clear" and be available to withdraw, the other person may still be able to withdraw the money from the other bank. A new teller or corrupt officer may approve the withdrawal since it is in pending status which then the other person cancels the wire transfer and the bank institution takes a monetary loss.

Essentially a confidence trick, a fraudster uses a company at their disposal to gain the bank's confidence, by posing as a genuine, profitable customer. To give the illusion of being a desired customer, the company regularly and repeatedly uses the bank to get payment from one or more of its customers. These payments are always made, as the customers in question are part of the fraud, actively paying any and all bills the bank attempts to collect. After the fraudster has gained the bank's trust, the company requests that the bank begin paying the company up front for bills it will collect from the customers later. Many banks will agree, but are not likely to go whole hog right away. So again, business continues as normal for the fraudulent company, its fraudulent customers, and the unwitting bank. As the bank grows more comfortable with the arrangement, it will trust the company more and more and be willing to give it larger and larger sums of money up front. Eventually, when the outstanding balance between the bank and the company is sufficiently large, the company and its customers disappear, taking the money the bank paid up front and leaving no-one to pay the bills issued by the bank.

Credit card fraud is widespread as a means of stealing from banks, merchants and clients.

A booster cheque is a fraudulent or bad cheque used to make a payment to a credit card account in order to "bust out" or raise the amount of available credit on otherwise-legitimate credit cards. The amount of the cheque is credited to the card account by the bank as soon as the payment is made, even though the cheque has not yet cleared. Before the bad cheque is discovered, the perpetrator goes on a spending spree or obtains cash advances until the newly-"raised" available limit on the card is reached. The original cheque then bounces, but by then it is already too late.

Often, the first indication that a victim's wallet has been stolen is a phone call from a credit card issuer asking if the person has gone on a spending spree; the simplest form of this theft involves stealing the card itself and charging a number of high-ticket items to it in the first few minutes or hours before it is reported as stolen.

A variant of this is to copy just the credit card numbers (instead of drawing attention by stealing the card itself) in order to use the numbers in online frauds.

This takes a number of forms, ranging from merchants copying clients' credit card numbers for use in later illegal activities or criminals using carbon copies from old mechanical card imprint machines to steal the info, to the use of tampered credit or debit card readers to copy the magnetic stripe from a payment card while a hidden camera captures the numbers on the face of the card.

Some fraudsters have attached fraudulent card stripe readers to publicly accessible ATMs, to gain unauthorised access to the contents of the magnetic stripe, as well as hidden cameras to illegally record users' authorisation codes. The data recorded by the cameras and fraudulent card stripe readers are subsequently used to produce duplicate cards that could then be used to make ATM withdrawals from the victims' accounts.

A criminal overdraft can result due to the account holder making a worthless or misrepresented deposit at an automated teller machine in order to obtain more cash than present in the account or to prevent a check from being returned due to non-sufficient funds. United States banking law makes the first $100 immediately available and it may be possible for much more uncollected funds to be lost by the bank the following business day before this type of fraud is discovered. The crime could also be perpetrated against another person's account in an "account takeover" or with a counterfeit ATM card, or an account opened in another person's name as part of an identity theft scam. The emergence of ATM deposit technology that scans currency and checks without using an envelope may prevent this type of fraud in the future.

Identity theft has become an increasing problem; the scam operates by obtaining information about an individual, then using the information to apply for identity cards, accounts and credit in that person's name. Often little more than name, parents' name, date and place of birth are sufficient to obtain a birth certificate; each document obtained then is used as identification in order to obtain more identity documents. Government-issued standard identification numbers such as "social security numbers" are also valuable to the fraudster.

Information may be obtained from insiders (such as dishonest bank or government employees), by fraudulent offers for employment or investments (in which the victim is asked for a long list of personal information) or by sending forged bank or taxation correspondence. Some fictitious tax forms which purported to have been sent by banks to clients in 2002 were:

- W-9095 Application Form for Certificate Status/Ownership for Withholding Tax
- W-8BEN Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding
- W-8888

The actual origin of these forms is neither the bank nor the taxman – they are sent by potential identity thieves and W-8888 doesn't exist, W-9095 is also fictitious (the real W-9 asks much less info) and W-8BEN is real but may have been tampered to add intrusive additional questions. The original forms on which these fakes were based are intended to collect information for income tax on income from deposits and investment.

In some cases, a name/SIN pair is needed to impersonate a citizen while working as an illegal immigrant but often the identity thieves are using the bogus identity documents in the commission of other crimes or even to hide from prosecution for past crimes. The use of a stolen identity for other frauds such as gaining access to bank accounts, credit cards, loans and fraudulent social benefit or tax refund claims is not uncommon.

Unsurprisingly, the perpetrators of such fraud have been known to take out loans and disappear with the cash.

The "prime bank" operation which claims to offer an urgent, exclusive opportunity to cash in on the best-kept secret in the banking industry, guaranteed deposits in "prime banks", "constitutional banks", "bank notes and bank-issued debentures from top 500 world banks", "bank guarantees and standby letters of credit" which generate spectacular returns at no risk and are "endorsed by the World Bank" or various national governments and central bankers. However, these official-sounding phrases and more are the hallmark of the so-called "prime bank" fraud; they may sound great on paper, but the guaranteed offshore investment with the vague claims of an easy 100% monthly return are all fictitious financial instruments intended to defraud individuals.

This is an old scam with a number of variants; the original scheme involved claiming to be a bank inspector, claiming that the bank suspects that one of its employees is stealing money and that to help catch the culprit the "bank inspector" needs the depositor to withdraw all of his or her money. At this point, the victim would be carrying a large amount of cash and can be targeted for the theft of these funds.

Other variants included claiming to be a prospective business partner with "the opportunity of a lifetime" then asking for access to cash "to prove that you trust me" or even claiming to be a new immigrant who carries all their money in cash for fear that the banks will steal it from them – if told by others that they keep their money in banks, they then ask the depositor to withdraw it to prove the bank hasn't stolen it.

Impersonation of officials has more recently become a way of stealing personal information for use in theft of identity frauds.

Phishing, also known as Internet fraud, operates by sending forged e-mail, impersonating an online bank, auction or payment site; the e-mail directs the user to a forged web site which is designed to look like the login to the legitimate site but which claims that the user must update personal info. The information thus stolen is then used in other frauds, such as theft of identity or online auction fraud.

A number of malicious "Trojan horse" programmes have also been used to snoop on Internet users while online, capturing keystrokes or confidential data in order to send it to outside sites.

Fake websites can trick you into downloading computer viruses that steal your personal information. Security messages are shown that tell you that you have viruses and need to download new software, by doing this you are tricked into downloading an actual virus.

The term "money laundering" dates back to the days of Al Capone; Money laundering has since been used to describe any scheme by which the true origin of funds is hidden or concealed.

Money laundering is the process by which large amounts of illegally obtained money (from drug trafficking, terrorist activity or other serious crimes) is given the appearance of having originated from a legitimate source.

Under federal law, bank fraud in the United States is defined, and made illegal, primarily by the Bank Fraud Statute in Title 18 of the U.S. Code. 18 U.S.C. § 1344 (Bank Fraud Statute) states:

> *Whoever knowingly executes, or attempts to execute, a scheme or artifice—*
> *(1) to defraud a financial institution; or*
> *(2) to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises;*
> *shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.*

State law may also criminalize the same, or similar acts.

The Bank Fraud Statute was passed following the Supreme Court's decision in *Williams v. United States*, 458 U.S. 279 (1982), in which the Court held that check-kiting schemes did not constitute making false statements to financial institutions (18 U.S.C. § 1014). Congress responded by passing the Bank Fraud Statute (18 U.S.C. § 1344). Section 1344 has subsequently been bolstered by the Financial Institutions Reform, Recovery and Enforcement Act of 1989 (FIRREA), Pub. L. No. 101-73, 103 Stat. 500.

The Bank Fraud Statute criminalizes federally check-kiting, check forging, non-disclosure on loan applications, diversion of funds, unauthorized use of automated teller machines (ATMs), credit card fraud, and other similar offenses. Section 1344 does not cover certain forms of money laundering, bribery, and passing bad checks. Other provisions cover these offenses.

In the United States, consumer liability for unauthorized electronic money transfers on debit cards is covered by Regulation-E of the Federal Deposit Insurance Corporation. The extent of consumer liability, as detailed in section 205.6, is determined by the speed with which the consumer notifies the bank. If the bank is notified within 2 business days, the consumer is liable for $50. Over two business days the consumer is liable for $500, and over 60 business days, the consumer liability is unlimited. In contrast, all major credit card companies have a zero liability policy, effectively eliminating consumer liability in the case of fraud.

A lawsuit concluded in 2012 in the city of Wenling, Jejiang province made news because the local court ordered the bank to fully reimburse a man who was the victim of card duplication.

The Commonwealth Fraud Control Framework outlines the preventions, detection, investigation and reporting obligations set by the Australian Government for fraud control. The framework includes three documents called The Fraud Rule, Fraud Policy and Fraud Guidance

The Fraud Rule is a legislative instrument binding all Commonwealth entities setting out the key requirements of fraud control.

The Fraud Policy is a government policy binding non-corporate Commonwealth entities setting out the procedural requirements for specific areas of fraud control such as investigations and reporting.

The Fraud Guidance preventing, detecting and dealing with fraud, supports best practice guidance for the Fraud Rule and Fraud Policy setting out the government's expectations for fraud control arrangements within all Commonwealth entities.

Other important acts and regulations in the Australian Government's fraud control framework include the:

- *CrimesAct 1914*, which sets out criminal offences against the Commonwealth, such as fraud
- *Criminal Code 1995*, which sets out criminal offences against the Commonwealth, such as fraudulent conduct
- *Public Service Act 1999* and the *Public Service Regulations 1999*, which provide for the establishment and management of the Australian Public Service and its employees
- *Proceeds of Crime Act 2002* and the *Proceeds of Crime Regulations 2002*, which provide for the confiscation of the proceeds of crime.

Differences between Customer Accounts, Small Business Accounts, and Business Accounts

Consumer bank accounts in the United States are protected under federal law.

Banks have the option of doing fraud detection either in real time or once every 24 hours. Since personal accounts are the responsibility of the banks, fraud detection for personal accounts is usually done in real time.

Although Visa and MasterCard both claim Zero Liability on their respective websites for Small Business Accounts, in reality, each bank can choose if they want to or not want hold by the Zero Liability guarantee. If an account does not specifically say "Small Business Account", it must be assumed that standard business account liability applies.

Even if the account says "Small Business Account", one must check with their respective bank to determine how much liability the account has.

Banks have the option of doing fraud detection either in real time or once every 24 hours. If a bank puts the liability of the Small Business Account onto the customer, it should be assumed that fraud detection is done once every 24 hours. If a bank assumes the liability for fraud on a Small Business Account, fraud detection could either be in real time or once every 24 hours. It is best to check with your bank to determine how often fraud detection is done.

MasterCard and Visa do not provide liability protection for business accounts. Since fraud is the responsibility of the customer, and not the bank, one should assume that fraud detection is done once every 24 hours. Check with your bank to determine if a business account has real time fraud detection.

Mortgage fraud

Mortgage fraud is a crime in which the intent is to materially misrepresent or omit information on a mortgage loan application in order to obtain a loan or to obtain a larger loan than could have been obtained had the lender or borrower known the truth.

In United States federal courts, mortgage fraud is prosecuted as wire fraud, bank fraud, mail fraud and money laundering, with penalties of up to thirty years imprisonment. As the incidence of mortgage fraud has risen over the past few years, states have also begun to enact their own penalties for mortgage fraud.

Mortgage fraud is not to be confused with predatory mortgage lending, which occurs when a consumer is misled or deceived by agents of the lender. However, predatory lending practices often co-exist with mortgage fraud.

Occupancy fraud: This occurs where the borrower wishes to obtain a mortgage to acquire an investment property, but states on the loan application that the borrower will occupy the property as the primary residence or as a second home. If undetected, the borrower typically obtains a lower interest rate than was warranted. Because lenders typically charge a higher interest rate for non-owner-occupied properties, which historically have higher delinquency rates, the lender receives insufficient return on capital and is over-exposed to loss relative to what was expected in the transaction. In addition, lenders allow larger loans on owner-occupied homes compared to loans for investment properties. When occupancy fraud occurs, it is likely that taxes on gains are not paid, resulting in additional fraud. It is considered fraud because the borrower has materially misrepresented the risk to the lender to obtain more favorable loan terms.

Income fraud: This occurs when a borrower overstates his/her income to qualify for a mortgage or for a larger loan amount. This was most often seen with so-called "stated income" mortgage loans (popularly referred to as "liar loans"), where the borrower, or a loan officer acting for a borrower with or without the borrower's knowledge, stated without verification the income needed to qualify for the loan. Because mortgage lenders today do not have "stated income" loans, income fraud is seen in traditional full-documentation loans where the borrower forges or alters an employer-issued Form W-2, tax returns and/or bank account records to provide support for the inflated income. All lenders obtain an official IRS transcript that must match the borrower provided tax returns. It is considered fraud because in most cases the borrower would not have qualified for the loan had the true income been disclosed. The "mortgage meltdown" was caused, in part, when large numbers of borrowers in areas of rapidly increasing home prices lied about their income, acquired

homes they could not afford, and then defaulted. Many of the past problems no longer exist.

Employment fraud: This occurs when a borrower claims self-employment in a non-existent company or claims a higher position (e.g., manager) in a real company, to provide justification for a fraudulent representation of the borrower's income.

Failure to disclose liabilities: Borrowers may conceal obligations, such as mortgage loans on other properties or newly acquired credit card debt, to reduce the amount of monthly debt declared on the loan application. This omission of liabilities artificially lowers the debt-to-income ratio, which is a key underwriting criterion used to determine eligibility for most mortgage loans. It is considered fraud because it allows the borrower to qualify for a loan which otherwise would not have been granted, or to qualify for a bigger loan than what would have been granted had the borrower's true debt been disclosed.

Fraud for profit: A complex scheme involving multiple parties, including mortgage lending professionals, in a financially motivated attempt to defraud the lender of large sums of money. Fraud for profit schemes frequently include a straw borrower whose credit report is used, a dishonest appraiser who intentionally and significantly overstates the value of the subject property, a dishonest settlement agent who might prepare two sets of HUD settlement statements or makes disbursements from loan proceeds which are not disclosed on the settlement statement, and a property owner, all in a coordinated attempt to obtain an inappropriately large loan. The parties involved share the ill-gotten gains and the mortgage eventually goes into default. In other cases, naive "investors" are lured into the scheme with the organizer's promise that the home will be repaired, repairs and/or renovations will be made, tenants will located, rents will be collected, mortgage payments made and profits will be split upon sale of the property, all without the active participation of the straw buyer. Once the loan is closed, the organizer disappears, no repairs are made nor renters found, and the "investor" is liable for paying the mortgage on a property that is not worth what is owed, leaving the "investor" financially ruined. If undetected, a bank may lend hundreds of thousands of dollars against a property that is actually worth far less and in large schemes with multiple transactions, banks may lend millions more than the properties are worth. The Robert Douglas Hartmann case is a notable example of this type of scheme. A detailed case study of the complex *United States v. Quintero-Lopez* case spans activity over 3 1/2 years (Bell, 2010).

Appraisal fraud: Occurs when a home's appraised value is deliberately overstated or understated. When overstated, more money can be obtained by the borrower in the form of a cash-out refinance, by the seller in a purchase transaction, or by the organizers of a for-profit mortgage fraud scheme. Appraisal fraud also includes cases

where the home's value is deliberately understated to get a lower price on a foreclosed home, or in a fraudulent attempt to induce a lender to decrease the amount owed on the mortgage in a loan modification. A dishonest appraiser may be involved in the preparation of the fraudulent appraisal, or an existing and accurate appraisal may be altered by someone with knowledge of graphic editing tools such as Adobe Photoshop. Appraisal Independence is current law.

Cash-back schemes: Occur where the true price of a property is illegally inflated to provide cash-back to transaction participants, most often the borrowers, who receive a "rebate" which is not disclosed to the lender. As a result, the lender lends too much, and the buyer pockets the overage or splits it with other participants, including the seller or the real estate agent. This scheme requires appraisal fraud to deceive the lender. "Get Rich Quick" real-estate gurus' courses frequently rely heavily on this mechanism for profitability.

Shotgunning: Occurs when multiple loans for the same home are obtained simultaneously for a total amount greatly in excess of the actual value of the property. These schemes leave lenders exposed to large losses because the subsequent mortgages are junior to the first mortgage to be recorded and the property value is insufficient for the subsequent lenders to collect against the property in foreclosure. The Matthew Cox and Robert Douglas Hartmann cases are the most notable example of this type of scheme. The result of this fraud is that lenders often litigate which has first priority to the property.

Working the gap: A technique which entails the excessive lien stacking knowingly executed on a specific property within an inordinately narrow timeframe, via the serial recording of multiple Deeds of Trust or Assignments of Note. When recording a legal document in the United States of America, a time gap exists between when the Deed of Trust is submitted to the Recorder of Deeds & when it actually shows up in the data. The precision timing technique of "working the gap" between the recording of a deed & its subsequent appearance in the recorder of deeds database is instrumental in propagating the perpetrator's deception. A title search done by any lender immediately prior to the respective loan, promissory note, & deed recording would thus erroneously fail to show the alternate liens concurrently in the queue. The goal of the perpetrator is the theft of funds from each lender by deceit, with all lenders simultaneously & erroneously believing their respective Deeds of Trust to be senior in position, when in actuality there can be only one. White-collar criminals who utilize this technique will frequently claim innocence based on clerical errors, bad record keeping, or other smokescreen excuses in an attempt to obfuscate the true coordination & intent inherent in this version of mortgage fraud. This "gaming" or exploitation of a structural weakness in the US legal system is a critical precursor to

"shotgunning" and considered white-collar crime when implemented in a systemic fashion.

Identity theft: Occurs when a person assumes the identity of another and uses that identity to obtain a mortgage without the knowledge or consent of the victim. In these schemes, the thieves disappear without making payments on the mortgage. The schemes are usually not discovered until the lender tries to collect from the victim, who may incur substantial costs trying to prove the theft of his/her identity.

Falsification of loan applications without the knowledge of the borrower : The loan applications are falsified without the knowledge of the borrower when the borrower actually will not qualify for a loan for various reasons. for example parties involved will make a commission out of the transaction. The business happens only if the loan application is falsified. For example, borrower applies for a loan stating monthly income of $2000 (but with this income $2000 per month the borrower will not qualify), however the broker or loan officer falsified the income documents and loan application that borrower earns a monthly income of $15,000. The loan gets approved the broker/loan officer etc. gets their commission. But the borrower struggles to repay the loan and defaults the loan eventually.

Mortgage fraud may be perpetrated by one or more participants in a loan transaction, including the borrower; a loan officer who originates the mortgage; a real estate agent, appraiser, a title or escrow representative or attorney; or by multiple parties as in the example of the fraud ring described above. Dishonest and unreputable stakeholders may encourage and assist borrowers in committing fraud because most participants are typically compensated only when a transaction closes.

During 2003 The Money Programme of the BBC in the UK uncovered systemic mortgage fraud throughout HBOS. The Money Programme found that during the investigation brokers advised the undercover researchers to lie on applications for self-certified mortgages from, among others, The Royal Bank of Scotland, The Mortgage Business and Birmingham Midshires Building Society.

In 2004, the FBI warned that mortgage fraud was becoming so rampant that the resulting "epidemic" of crimes could trigger a massive financial crisis. According to a December 2005 press release from the FBI, "mortgage fraud is one of the fastest growing white collar crimes in the United States".

The number of FBI agents assigned to mortgage-related crimes increased by 50 percent between 2007 and 2008. In June 2008, The FBI stated that its mortgage fraud caseload has doubled in the past three years to more than 1,400 pending cases. Between March 1 and June 18, 2008, 406 people were arrested for mortgage

fraud in an FBI sting across the country. People arrested include buyers, sellers and others across the wide-ranging mortgage industry.

In May 2009, the Fraud Enforcement and Recovery Act of 2009, or **FERA**, Pub.L. 111–21, 123 Stat. 1617, S. 386, public law in the United States, was enacted. The law takes a number of steps to enhance criminal enforcement of federal fraud laws, especially regarding financial institutions, mortgage fraud, and securities fraud or commodities fraud.

Significant to note, Section 3 of the Act authorized additional funding to detect and prosecute fraud at various federal agencies, specifically:

- $165,000,000 to the Department of Justice,
- $30,000,000 each to the Postal Inspection Service and the Office of the Inspector General at the United States Department of Housing and Urban Development (HUD/OIG)
- $20,000,000 to the Secret Service
- $21,000,000 to the Securities and Exchange Commission

These authorizations were made for the federal fiscal years beginning October 1, 2009 and 2010, after which point they expire, and are in addition to the previously authorized budgets for these agencies.

Money laundering

Money laundering is the act of concealing the transformation of profits from illegal activities and corruption into ostensibly "legitimate" assets. The dilemma of illicit activities is accounting for the origin of the proceeds of such activities without raising the suspicion of law enforcement agencies. Accordingly, considerable time and effort is put into devising strategies which enable the safe use of those proceeds without raising unwanted suspicion. Implementing such strategies is generally called money laundering. After money has been suitably laundered or “cleaned”, it can be used in the mainstream economy for accumulation of wealth, such as acquisitions of properties, or otherwise spent. Law enforcement agencies of many jurisdictions have set up sophisticated systems in an effort to detect suspicious transactions or activities, and many have set up international cooperative arrangements to assist each other in these endeavours.

In a number of legal and regulatory systems, the term money laundering has become conflated with other forms of financial and business crime, and is sometimes used more generally to include misuse of the financial system (involving things such as securities, digital currencies, credit cards, and traditional currency), including terrorism financing and evasion of international sanctions. Most anti-money laundering laws openly conflate money laundering (which is concerned with *source* of funds) with terrorism financing (which is concerned with *destination* of funds) when regulating the financial system.

Some countries treat obfuscation of sources of money as also constituting money laundering, whether it is intentional or by merely using financial systems or services that do not identify or track sources or destinations. Other countries define money laundering in such a way as to include money from activity that *would have been* a crime in that country, even if the activity was legal where the actual conduct occurred.

The concept of money laundering regulations goes back to ancient times and is intertwined with the development of money and banking. Money laundering is first seen with individuals hiding wealth from the state to avoid taxation or confiscation or a combination of both.

In China, merchants around 2000 BCE would hide their wealth from rulers who would simply take it from them and banish them. In addition to hiding it, they would move it and invest it in businesses in remote provinces or even outside China.

Over the millennia many rulers and states imposed rules that would take wealth from their citizens and this led to the development of offshore banking and tax evasion.

One of the enduring methods has been the use of parallel banking or Informal value transfer systems such as hawala that allowed people to move money out of the country avoiding state scrutiny.

In the 20th century, the seizing of wealth again became popular when it was seen as an additional crime prevention tool. The first time was during the period of Prohibition in the United States during the 1930s. This saw a new emphasis by the state and law enforcement agencies to track and confiscate money. Organized crime received a major boost from Prohibition and a large source of new funds that were obtained from illegal sales of alcohol.

In the 1980s, the war on drugs led governments again to turn to money-laundering rules in an attempt to seize proceeds of drug crimes in order to catch the organizers and individuals running drug empires. It also had the benefit from a law enforcement point of view of turning rules of evidence upside down. Law enforcers normally have to prove an individual is guilty to get a conviction. But with money laundering laws, money can be confiscated and it is up to the individual to prove that the source of funds is legitimate if they want the funds back. This makes it much easier for law enforcement agencies and provides for much lower burdens of proof.

The September 11 attacks in 2001, which led to the Patriot Act in the US and similar legislation worldwide, led to a new emphasis on money laundering laws to combat terrorism financing. The Group of Seven (G7) nations used the Financial Action Task Force on Money Laundering to put pressure on governments around the world to increase surveillance and monitoring of financial transactions and share this information between countries. Starting in 2002, governments around the world upgraded money laundering laws and surveillance and monitoring systems of financial transactions. Anti money laundering regulations have become a much larger burden for financial institutions and enforcement has stepped up significantly. During 2011–2015 a number of major banks faced ever-increasing fines for breaches of money laundering regulations. This included HSBC, which was fined $1.9 billion in December 2012, and BNP Paribas, which was fined $8.9 billion in July 2014 by the US government. Many countries introduced or strengthened border controls on the amount of cash that can be carried and introduced central transaction reporting systems where all financial institutions have to report all financial transactions electronically. For example, in 2006, Australia set up the AUSTRAC system and required the reporting of all financial transactions.

The conversation or Transfer of property, the concealment or disguising of the nature of the proceeds, the acquisition, possession or use of property, knowing that these are derived from criminal activity and participate or assist the movement of funds to make the proceeds appear legitimate is money laundering.

Money obtained from certain crimes, such as extortion, insider trading, drug trafficking, and illegal gambling is "dirty" and needs to be "cleaned" to appear to have been derived from legal activities, so that banks and other financial institutions will deal with it without suspicion. Money can be laundered by many methods which vary in complexity and sophistication.

Money laundering involves three steps: The first involves introducing cash into the financial system by some means ("placement"); the second involves carrying out complex financial transactions to camouflage the illegal source of the cash ("layering"); and finally, acquiring wealth generated from the transactions of the illicit funds ("integration"). Some of these steps may be omitted, depending upon the circumstances. For example, non-cash proceeds that are already in the financial system would not need to be placed.

According to the United States Treasury Department:

Money laundering is the process of making illegally-gained proceeds (i.e., "dirty money") appear legal (i.e., "clean"). Typically, it involves three steps: placement, layering, and integration. First, the illegitimate funds are furtively introduced into the legitimate financial system. Then, the money is moved around to create confusion, sometimes by wiring or transferring through numerous accounts. Finally, it is integrated into the financial system through additional transactions until the "dirty money" appears "clean."

Money laundering can take several forms, although most methods can be categorized into one of a few types. These include "bank methods, smurfing [also known as structuring], currency exchanges, and double-invoicing".

- Structuring: Often known as *smurfing*, this is a method of placement whereby cash is broken into smaller deposits of money, used to defeat suspicion of money laundering and to avoid anti-money laundering reporting requirements. A sub-component of this is to use smaller amounts of cash to purchase bearer instruments, such as money orders, and then ultimately deposit those, again in small amounts.
- Bulk cash smuggling: This involves physically smuggling cash to another jurisdiction and depositing it in a financial institution, such as an offshore bank, with greater bank secrecy or less rigorous money laundering enforcement.
- Cash-intensive businesses: In this method, a business typically expected to receive a large proportion of its revenue as cash uses its accounts to deposit criminally derived cash. Such enterprises often operate openly and in doing so generate cash revenue from incidental legitimate business in addition to the illicit cash – in such cases the business will usually claim all cash received as

legitimate earnings. Service businesses are best suited to this method, as such enterprises have little or no variable costs and/or a large ratio between revenue and variable costs, which makes it difficult to detect discrepancies between revenues and costs. Examples are parking structures, strip clubs, tanning salons, car washes, arcades, bars, restaurants, and casinos.

- Trade-based laundering: This involves under- or over-valuing invoices to disguise the movement of money.
- Shell companies and trusts: Trusts and shell companies disguise the true owners of money. Trusts and corporate vehicles, depending on the jurisdiction, need not disclose their true owner. Sometimes referred to by the slang term *rathole*, though that term usually refers to a person acting as the fictitious owner rather than the business entity.
- Round-tripping: Here, money is deposited in a controlled foreign corporation offshore, preferably in a tax haven where minimal records are kept, and then shipped back as a foreign direct investment, exempt from taxation. A variant on this is to transfer money to a law firm or similar organization as funds on account of fees, then to cancel the retainer and, when the money is remitted, represent the sums received from the lawyers as a legacy under a will or proceeds of litigation.
- Bank capture: In this case, money launderers or criminals buy a controlling interest in a bank, preferably in a jurisdiction with weak money laundering controls, and then move money through the bank without scrutiny.
- Casinos: In this method, an individual walks into a casino and buys chips with illicit cash. The individual will then play for a relatively short time. When the person cashes in the chips, they will expect to take payment in a check, or at least get a receipt so they can claim the proceeds as gambling winnings.
- Other gambling: Money is spent on gambling, preferably on high odds games. One way to minimize risk with this method is to bet on every possible outcome of some event that has many possible outcomes, so no outcome(s) have short odds, and the bettor will lose only the vigorish and will have one or more winning bets that can be shown as the source of money. The losing bets will remain hidden.
- Real estate: Someone purchases real estate with illegal proceeds and then sells the property. To outsiders, the proceeds from the sale look like legitimate income. Alternatively, the price of the property is manipulated: the seller agrees to a contract that underrepresents the value of the property, and receives criminal proceeds to make up the difference.
- Black salaries: A company may have unregistered employees without written contracts and pay them cash salaries. Dirty money might be used to pay them.
- Tax amnesties: For example, those that legalize unreported assets and cash in tax havens.

- Life insurance business: Assignment of policies to unidentified third parties and for which no plausible reasons can be ascertained.
- Many regulatory and governmental authorities issue estimates each year for the amount of money laundered, either worldwide or within their national economy. In 1996, a spokesperson for the IMF estimated that 2–5% of the worldwide global economy involved laundered money. The Financial Action Task Force on Money Laundering (FATF), an intergovernmental body set up to combat money laundering, stated, "Overall, it is absolutely impossible to produce a reliable estimate of the amount of money laundered and therefore the FATF does not publish any figures in this regard." Academic commentators have likewise been unable to estimate the volume of money with any degree of assurance. Various estimates of the scale of global money laundering are sometimes repeated often enough to make some people regard them as factual—but no researcher has overcome the inherent difficulty of measuring an actively concealed practice.
- Regardless of the difficulty in measurement, the amount of money laundered each year is in the billions of US dollars and poses a significant policy concern for governments. As a result, governments and international bodies have undertaken efforts to deter, prevent, and apprehend money launderers. Financial institutions have likewise undertaken efforts to prevent and detect transactions involving dirty money, both as a result of government requirements and to avoid the reputational risk involved. Issues relating to money laundering have existed as long as there have been large scale criminal enterprises. Modern anti-money laundering laws have developed along with the modern War on Drugs. In more recent times anti-money laundering legislation is seen as adjunct to the financial crime of terrorist financing in that both crimes usually involve the transmission of funds through the financial system .
- In theory, electronic money should provide as easy a method of transferring value without revealing identity as untracked banknotes, especially wire transfers involving anonymity-protecting numbered bank accounts. In practice, however, the record-keeping capabilities of Internet service providers and other network resource maintainers tend to frustrate that intention. While some cryptocurrencies under recent development have aimed to provide for more possibilities of transaction anonymity for various reasons, the degree to which they succeed—and, in consequence, the degree to which they offer benefits for money laundering efforts—is controversial. Solutions such as ZCash and Monero are examples of cryptocurrencies that provide unlinkable anonymity via proofs and/or obfuscation of information (Ring signatures). Such currencies could find use in online illicit services.
- In 2013, Jean-Loup Richet, a research fellow at ESSEC ISIS, surveyed new techniques that cybercriminals were using in a report written for the United

Nations Office on Drugs and Crime. A common approach was to use a digital currency exchanger service which converted dollars into a digital currency called Liberty Reserve, and could be sent and received anonymously. The receiver could convert the Liberty Reserve currency back into cash for a small fee. In May 2013, the US authorities shut down Liberty Reserve charging its founder and various others with money laundering.

- Another increasingly common way of laundering money is to use online gaming. In a growing number of online games, such as *Second Life* and *World of Warcraft*, it is possible to convert money into virtual goods, services, or virtual cash that can later be converted back into money.

Reverse money laundering is a process that disguises a legitimate source of funds that are to be used for illegal purposes. It is usually perpetrated for the purpose of financing terrorism but can be also used by criminal organizations that have invested in legal businesses and would like to withdraw legitimate funds from official circulation. Unaccounted cash received via disguising financial transactions is not included in official financial reporting and could be used to evade taxes, hand in bribes and pay "under-the-table" salaries. For example, in an affidavit filed 24 March 2014 in United States District Court, Northern California, San Francisco Division, FBI special agent Emmanuel V. Pascau alleged that several people associated with the Chee Kung Tong organization, and California State Senator Leland Yee, engaged in reverse money laundering activities.

The problem of such fraudulent encashment practices (*obnalichka* in Russian) has become acute in Russia and other countries of the former Soviet Union. The Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) reported that the Russian Federation, Ukraine, Turkey, Serbia, Kyrgyzstan, Uzbekistan, Armenia and Kazakhstan have encountered a substantial shrinkage of tax base and shifting money supply balance in favor of cash. These processes have complicated planning and management of the economy and contributed to the growth of the shadow economy .

Anti-money laundering (AML) is a term mainly used in the financial and legal industries to describe the legal controls that require financial institutions and other regulated entities to prevent, detect, and report money laundering activities. Anti-money laundering guidelines came into prominence globally as a result of the formation of the Financial Action Task Force (FATF) and the promulgation of an international framework of anti-money laundering standards. These standards began to have more relevance in 2000 and 2001, after FATF began a process to publicly

identify countries that were deficient in their anti-money laundering laws and international cooperation, a process colloquially known as "name and shame".

An effective AML program requires a jurisdiction to criminalise money laundering, giving the relevant regulators and police the powers and tools to investigate; be able to share information with other countries as appropriate; and require financial institutions to identify their customers, establish risk-based controls, keep records, and report suspicious activities.

The elements of the crime of money laundering are set forth in the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances and Convention against Transnational Organized Crime. It is defined as knowingly engaging in a financial transaction with the proceeds of a crime for the purpose of concealing or disguising the illicit origin of the property from governments.

While banks operating in the same country generally have to follow the same anti-money laundering laws and regulations, financial institutions all structure their anti-money laundering efforts slightly differently. Today, most financial institutions globally, and many non-financial institutions, are required to identify and report transactions of a suspicious nature to the financial intelligence unit in the respective country. For example, a bank must verify a customer's identity and, if necessary, monitor transactions for suspicious activity. This is often termed as "know your customer". This means knowing the identity of the customer and understanding the kinds of transactions in which the customer is likely to engage. By knowing one's customers, financial institutions can often identify unusual or suspicious behaviour, termed anomalies, which may be an indication of money laundering.

Bank employees, such as tellers and customer account representatives, are trained in anti-money laundering and are instructed to report activities that they deem suspicious. Additionally, anti-money laundering software filters customer data, classifies it according to level of suspicion, and inspects it for anomalies. Such anomalies include any sudden and substantial increase in funds, a large withdrawal, or moving money to a bank secrecy jurisdiction. Smaller transactions that meet certain criteria may also be flagged as suspicious. For example, structuring can lead to flagged transactions. The software also flags names on government "blacklists" and transactions that involve countries hostile to the host nation. Once the software has mined data and flagged suspect transactions, it alerts bank management, who must then determine whether to file a report with the government.

The financial services industry has become more vocal about the rising costs of anti-money laundering regulation and the limited benefits that they claim it brings. One

commentator wrote that "[w]ithout facts, [anti-money laundering] legislation has been driven on rhetoric, driving by ill-guided activism responding to the need to be "seen to be doing something" rather than by an objective understanding of its effects on predicate crime. The social panic approach is justified by the language used—we talk of the battle against terrorism or the war on drugs".*The Economist* magazine has become increasingly vocal in its criticism of such regulation, particularly with reference to countering terrorist financing, referring to it as a "costly failure", although it concedes that other efforts (like reducing identity and credit card fraud) may still be effective at combating money laundering.

There is no precise measurement of the costs of regulation balanced against the harms associated with money laundering, and given the evaluation problems involved in assessing such an issue, it is unlikely that the effectiveness of terror finance and money laundering laws could be determined with any degree of accuracy. *The Economist* estimated the annual costs of anti-money laundering efforts in Europe and North America at US$5 billion in 2003, an increase from US$700 million in 2000. Government-linked economists have noted the significant negative effects of money laundering on economic development, including undermining domestic capital formation, depressing growth, and diverting capital away from development. Because of the intrinsic uncertainties of the amount of money laundered, changes in the amount of money laundered, and the cost of anti-money laundering systems, it is almost impossible to tell which anti-money laundering systems work and which are more or less cost effective.

Besides economic costs to implement anti-money-laundering laws, improper attention to data protection practices may entail disproportionate costs to individual privacy rights. In June 2011, the data-protection advisory committee to the European Union issued a report on data protection issues related to the prevention of money laundering and terrorist financing, which identified numerous transgressions against the established legal framework on privacy and data protection. The report made recommendations on how to address money laundering and terrorist financing in ways that safeguard personal privacy rights and data protection laws. In the United States, groups such as the American Civil Liberties Union have expressed concern that money laundering rules require banks to report on their own customers, essentially conscripting private businesses "into agents of the surveillance state".

Many countries are obligated by various international instruments and standards, such as the 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, the 2000 Convention against Transnational Organized Crime, the 2003 United Nations Convention against Corruption, and the recommendations of the 1989 Financial Action Task Force on Money Laundering (FATF) to enact and enforce money laundering laws in an effort to stop

narcotics trafficking, international organised crime, and corruption. Mexico, which has faced a significant increase in violent crime, established anti-money laundering controls in 2013 to curb the underlying crime issue.

Formed in 1989 by the G7 countries, the Financial Action Task Force on Money Laundering (FATF) is an intergovernmental body whose purpose is to develop and promote an international response to combat money laundering. The FATF Secretariat is housed at the headquarters of the OECD in Paris. In October 2001, FATF expanded its mission to include combating the financing of terrorism. FATF is a policy-making body that brings together legal, financial, and law enforcement experts to achieve national legislation and regulatory AML and CFT reforms. As of 2014 its membership consists of 36 countries and territories and two regional organizations. FATF works in collaboration with a number of international bodies and organizations. These entities have observer status with FATF, which does not entitle them to vote, but permits them full participation in plenary sessions and working groups.

FATF has developed 40 recommendations on money laundering and 9 special recommendations regarding terrorist financing. FATF assesses each member country against these recommendations in published reports. Countries seen as not being sufficiently compliant with such recommendations are subjected to financial sanctions.

FATF's three primary functions with regard to money laundering are:

1. Monitoring members' progress in implementing anti-money laundering measures,
2. Reviewing and reporting on laundering trends, techniques, and countermeasures, and
3. Promoting the adoption and implementation of FATF anti-money laundering standards globally.

The FATF currently comprises 34 member jurisdictions and 2 regional organisations, representing most major financial centres in all parts of the globe.

The United Nations Office on Drugs and Crime maintains the *International Money Laundering Information Network*, a website that provides information and software for anti-money laundering data collection and analysis. The World Bank has a website that provides policy advice and best practices to governments and the private sector on anti-money laundering issues.

Many jurisdictions adopt a list of specific predicate crimes for money laundering prosecutions, while others criminalize the proceeds of any serious crimes.

The Financial Transactions and Reports Analysis Center of Afghanistan (FinTRACA) was established as a Financial Intelligence Unit (FIU) under the Anti Money Laundering and Proceeds of Crime Law passed by decree late in 2004. The main purpose of this law is to protect the integrity of the Afghan financial system and to gain compliance with international treaties and conventions. The Financial Intelligence Unit is a semi-independent body that is administratively housed within the Central Bank of Afghanistan (Da Afghanistan Bank). The main objective of FinTRACA is to deny the use of the Afghan financial system to those who obtained funds as the result of illegal activity, and to those who would use it to support terrorist activities.

To meet its objectives, the FinTRACA collects and analyzes information from a variety of sources. These sources include entities with legal obligations to submit reports to the FinTRACA when a suspicious activity is detected, as well as reports of cash transactions above a threshold amount specified by regulation. Also, FinTRACA has access to all related Afghan government information and databases. When the analysis of this information supports the supposition of illegal use of the financial system, the FinTRACA works closely with law enforcement to investigate and prosecute the illegal activity. FinTRACA also cooperates internationally in support of its own analyses and investigations and to support the analyses and investigations of foreign counterparts, to the extent allowed by law. Other functions include training of those entities with legal obligations to report information, development of laws and regulations to support national-level AML objectives, and international and regional cooperation in the development of AML typologies and countermeasures.

Australia has adopted a number of strategies to combat money laundering, which mirror those of a majority of western countries. The Australian Transaction Reports and Analysis Centre (AUSTRAC) is Australia's financial intelligence unit to combat money laundering and terrorism financing, which requires financial institutions and other 'cash dealers' in Australia to report to it suspicious cash or other transactions and other specific information. The Attorney-General's Department maintains a list of outlawed terror organisations. It is an offense to materially support or be supported by such organisations. It is an offence to open a bank account in Australia in a false name, and rigorous procedures must be followed when new bank accounts are opened.

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) is the principal legislative instrument, although there are also offence provisions contained in Division 400 of the *Criminal Code Act 1995* (Cth). Upon its introduction, it was intended that the AML/CTF Act would be further amended by a second tranche of reforms extending to designated non-financial businesses and professions (DNFBPs) including, inter alia, lawyers, accountants, jewellers and real estate agents; however, those further reforms have yet to be progressed.

The *Proceeds of Crime Act 1987* (Cth) imposes criminal penalties on a person who engages in money laundering, and allows for confiscation of property. The principal objects of the Act are set out in s.3(1):

- to deprive persons of the proceeds of, and benefits derived from the commission of offences,
- to provide for the forfeiture of property used in or in connection with the commission of such offences, and
- to enable law enforcement authorities to effectively trace such proceeds, benefits and property.

The first anti-money laundering legislation in Bangladesh was the *Money Laundering Prevention Act, 2002*. It was replaced by the *Money Laundering Prevention Ordinance 2008*. Subsequently, the ordinance was repealed by the *Money Laundering Prevention Act, 2009*. In 2012, government again replace it with the *Money Laundering Prevention Act, 2012*

In terms of section 2, "Money Laundering means – (i) knowingly moving, converting, or transferring proceeds of crime or property involved in an offence for the following purposes:- (1) concealing or disguising the illicit nature, source, location, ownership or control of the proceeds of crime; or (2) assisting any person involved in the commission of the predicate offence to evade the legal consequences of such offence; (ii) smuggling money or property earned through legal or illegal means to a foreign country; (iii) knowingly transferring or remitting the proceeds of crime to a foreign country or remitting or bringing them into Bangladesh from a foreign country with the intention of hiding or disguising its illegal source; or (iv) concluding or attempting to conclude financial transactions in such a manner so as to reporting requirement under this Act may be avoided;(v) converting or moving or transferring property with the intention to instigate or assist for committing a predicate offence; (vi) acquiring, possessing or using any property, knowing that such property is the proceeds of a predicate offence; (vii) performing such activities so as to the illegal source of the proceeds of crime may be concealed or disguised; (viii) participating in, associating with, conspiring, attempting, abetting, instigate or counsel to commit any offences mentioned above.

To prevent these Illegal uses of money, the Bangladesh government has introduced the Money Laundering Prevention Act. The Act was last amended in the year 2009 and all the financial institutes are following this act. Till today there are 26 circulars issued by Bangladesh Bank under this act. To prevent money laundering, a banker must do the following:

- While opening a new account, the account opening form should be duly filled up by all the information of the customer.
- The KYC must be properly filled.
- The Transaction Profile (TP) is mandatory for a client to understand his/her transactions. If needed, the TP must be updated at the client's consent.
- All other necessary papers should be properly collected along with the National ID card.
- If any suspicious transaction is noticed, the Branch Anti Money Laundering Compliance Officer (BAMLCO) must be notified and accordingly the Suspicious Transaction Report (STR) must be filled out.
- The cash department should be aware of the transactions. It must be noted if suddenly a big amount of money is deposited in any account. Proper documents are required if any client does this type of transaction.
- Structuring, over/ under invoicing is another way to do money laundering. The foreign exchange department should look into this matter cautiously.
- If any account has a transaction over 1 million taka in a single day, it must be reported in a cash transaction report (CTR).
- All bank officials must go through all the 26 circulars and use them.

In 1991, the Proceeds of Crime (Money Laundering) Act was brought into force in Canada to give legal effect to the former FATF Forty Recommendations by establishing record keeping and client identification requirements in the financial sector to facilitate the investigation and prosecution of money laundering offences under the Criminal Code and the Controlled Drugs and Substances Act.

In 2000, the Proceeds of Crime (Money Laundering) Act was amended to expand the scope of its application and to establish a financial intelligence unit with national control over money laundering, namely FINTRAC.

In December 2001, the scope of the Proceeds of Crime (Money Laundering) Act was again expanded by amendments enacted under the Anti-Terrorism Act with the objective of deterring terrorist activity by cutting off sources and channels of funding used by terrorists in response to 9/11. The Proceeds of Crime (Money Laundering) Act was renamed the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.

In December 2006, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act was further amended, in part, in response to pressure from the FATF for Canada to tighten its money laundering and financing of terrorism legislation. The amendments expanded the client identification, record-keeping and reporting

requirements for certain organizations and included new obligations to report attempted suspicious transactions and outgoing and incoming international electronic fund transfers, undertake risk assessments and implement written compliance procedures in respect of those risks.

The amendments also enabled greater money laundering and terrorist financing intelligence-sharing among enforcement agencies.

In Canada, casinos, money service businesses, notaries, accountants, banks, securities brokers, life insurance agencies, real estate salespeople and dealers in precious metals and stones are subject to the reporting and record keeping obligations under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.

The fourth and latest iteration of the EU's anti-money laundering directive (AMLD IV) was published on 5 June 2015, after clearing its last legislative stop at the European Parliament. The new directive brings the EU's anti-money laundering laws more in line with the US's, which is welcome news for financial institutions that are operating in both jurisdictions.

Lack of harmonization in AML requirements between the US and EU has complicated the compliance efforts of global institutions that are looking to standardize the Know Your Customer (KYC) component of their AML programs across key jurisdictions. AMLD IV promises to better align the AML regimes by adopting a more risk-based approach compared to its predecessor, AMLD III.

Certain components of the directive, however, go beyond current requirements in both the EU and US, imposing new implementation challenges on banks. For instance, more public officials are brought within the scope of the directive, and EU member states are required to establish new registries of "beneficial owners" (i.e., those who ultimately own or control each company) which will impact banks. AMLD IV became effective 25 June 2015.

In 2002, the Parliament of India passed an act called the Prevention of Money Laundering Act, 2002. The main objectives of this act are to prevent money-laundering as well as to provide for confiscation of property either derived from or involved in, money-laundering.

Section 12 (1) describes the obligations that banks, other financial institutions, and intermediaries have to

(a) Maintain records that detail the nature and value of transactions, whether such transactions comprise a single transaction or a series of connected transactions, and where these transactions take place within a month.
(b) Furnish information on transactions referred to in clause (a) to the Director within the time prescribed, including records of the identity of all its clients.

Section 12 (2) prescribes that the records referred to in sub-section (1) as mentioned above, must be maintained for ten years after the transactions finished. It is handled by the Indian Income Tax Department.

The provisions of the Act are frequently reviewed and various amendments have been passed from time to time.

Most money laundering activities in India are through political parties, corporate companies and the shares market. These are investigated by the Enforcement Directorate and Indian Income Tax Department. According to Government of India, out of the total tax arrears of ₹2,480 billion (US$38 billion) about ₹1,300 billion (US$20 billion) pertain to money laundering and securities scam cases.

Bank accountants must record all transactions over Rs. 1 million and maintain such records for 10 years. Banks must also make cash transaction reports (CTRs) and suspicious transaction reports over Rs. 1 million within 7 days of initial suspicion. They must submit their reports to the Enforcement Directorate and Income Tax Department.

Singapore's legal framework for combating money laundering is contained in a patchwork of legal instruments, the main elements of which are:

- The Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA). This statute criminalises money laundering and imposes the requirement for persons to file suspicious transaction reports (STRs) and make a disclosure whenever physical currency or goods exceeding S$20,000 are carried into or out of Singapore.
- The Mutual Assistance in Criminal Matters Act (MACMA). This statute sets out the framework for mutual legal assistance in criminal matters.
- Legal instruments issued by regulatory agencies (such as the Monetary Authority of Singapore (MAS), in relation to financial institutions (FIs)) imposing requirements to conduct customer due diligence (CDD).

The term 'money laundering' is not used as such within the CDSA. Part VI of the CDSA criminalises the laundering of proceeds generated by criminal conduct and drug tracking via the following offences:

- The assistance of another person in retaining, controlling or using the benefits of drug dealing or criminal conduct under an arrangement (whether by concealment, removal from jurisdiction, transfer to nominees or otherwise) [section 43(1)/44(1)].
- The concealment, conversion, transfer or removal from the jurisdiction, or the acquisition, possession or use of benefits of drug dealing or criminal conduct [section 46(1)/47(1)].
- The concealment, conversion, transfer or removal from the jurisdiction of another person's benefits of drug dealing or criminal conduct [section 46(2)/47(2)].
- The acquirement, possession or use of another person's benefits of drug dealing or criminal conduct [section 46(3)/47(3)].

Money laundering and terrorist funding legislation in the UK is governed by four Acts of primary legislation:-

- Terrorism Act 2000
- Anti-terrorism, Crime and Security Act 2001
- Proceeds of Crime Act 2002
- Serious Organised Crime and Police Act 2005
- Money Laundering Regulations 2007
- Money Laundering Regulation, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

Money Laundering Regulations are designed to protect the UK financial system, as well as preventing and detecting crime. If a business is covered by these regulations then controls are put in place to prevent it being used for money laundering.

The Proceeds of Crime Act 2002 contains the primary UK anti-money laundering legislation, including provisions requiring businesses within the "regulated sector" (banking, investment, money transmission, certain professions, etc.) to report to the authorities suspicions of money laundering by customers or others.

Money laundering is broadly defined in the UK. In effect any handling or involvement with any proceeds of any crime (or monies or assets representing the proceeds of crime) can be a money laundering offence. An offender's possession of the proceeds of his own crime falls within the UK definition of money laundering. The definition also covers activities within the traditional definition of money laundering, as a process that conceals or disguises the proceeds of crime to make them appear legitimate.

Unlike certain other jurisdictions (notably the US and much of Europe), UK money laundering offences are not limited to the proceeds of serious crimes, nor are there any monetary limits. Financial transactions need no money laundering design or purpose for UK laws to consider them a money laundering offence. A money laundering offence under UK legislation need not even involve money, since the money laundering legislation covers assets of any description. In consequence, any person who commits an acquisitive crime (i.e., one that produces some benefit in the form of money or an asset of any description) in the UK inevitably also commits a money laundering offence under UK legislation.

This applies also to a person who, by criminal conduct, evades a liability (such as a taxation liability)—which lawyers call "obtaining a pecuniary advantage"—as he is deemed thereby to obtain a sum of money equal in value to the liability evaded.

The principal money laundering offences carry a maximum penalty of 14 years' imprisonment.

Secondary regulation is provided by the Money Laundering Regulations 2003, which was replaced by the Money Laundering Regulations 2007. They are directly based on the EU directives 91/308/EEC, 2001/97/EC and 2005/60/EC.

One consequence of the Act is that solicitors, accountants, tax advisers, and insolvency practitioners who suspect (as a consequence of information received in the course of their work) that their clients (or others) have engaged in tax evasion or other criminal conduct that produced a benefit, now must report their suspicions to the authorities (since these entail suspicions of money laundering). In most circumstances it would be an offence, "tipping-off", for the reporter to inform the subject of his report that a report has been made. These provisions do not however require disclosure to the authorities of information received by certain professionals in privileged circumstances or where the information is subject to legal professional privilege. Others that are subject to these regulations include financial institutions, credit institutions, estate agents (which includes chartered surveyors), trust and company service providers, high value dealers (who accept cash equivalent to €15,000 or more for goods sold), and casinos.

Professional guidance (which is submitted to and approved by the UK Treasury) is provided by industry groups including the Joint Money Laundering Steering Group, the Law Society. and the Consultative Committee of Accountancy Bodies (CCAB). However, there is no obligation on banking institutions to routinely report monetary deposits or transfers above a specified value. Instead reports must be made of all suspicious deposits or transfers, irrespective of their value.

The reporting obligations include reporting suspicious gains from conduct in other countries that would be criminal if it took place in the UK. Exceptions were later added for certain activities legal where they took place, such as bullfighting in Spain.

More than 200,000 reports of suspected money laundering are submitted annually to authorities in the UK (there were 240,582 reports in the year ended 30 September 2010. This was an increase from the 228,834 reports submitted in the previous year). Most of these reports are submitted by banks and similar financial institutions (there were 186,897 reports from the banking sector in the year ended 30 September 2010).

Although 5,108 different organisations submitted suspicious activity reports to the authorities in the year ended 30 September 2010, just four organisations submitted approximately half of all reports, and the top 20 reporting organisations accounted for three-quarters of all reports.

The offence of failing to report a suspicion of money laundering by another person carries a maximum penalty of 5 years' imprisonment.

Bureaux de change

All UK *Bureaux de change* are registered with Her Majesty's Revenue and Customs, which issues a trading licence for each location. Bureaux de change and money transmitters, such as Western Unionoutlets, in the UK fall within the "regulated sector" and are required to comply with the Money Laundering Regulations 2007. Checks can be carried out by HMRC on all Money Service Businesses.

In South Africa, the Financial Intelligence Centre Act (2001) and subsequent amendments have added responsibilities to the FSB to combat money laundering.

United States

The approach in the United States to stopping money laundering is usually broken into two areas: preventive (regulatory) measures and criminal measures.

In an attempt to prevent dirty money from entering the U.S. financial system in the first place, the United States Congress passed a series of laws, starting in 1970, collectively known as the Bank Secrecy Act(BSA). These laws, contained in sections 5311 through 5332 of Title 31 of the United States Code, require financial institutions, which under the current definition include a broad array of entities, including banks, credit card companies, life insurers, money service businesses and broker-dealers in securities, to report certain transactions to the United States Department of the

Treasury. Cash transactions in excess of a certain amount must be reported on a currency transaction report (CTR), identifying the individual making the transaction as well as the source of the cash. The law originally required all transactions of US$5,000 or more to be reported, but due to excessively high levels of reporting the threshold was raised to US$10,000. The U.S. is one of the few countries in the world to require reporting of all cash transactions over a certain limit, although certain businesses can be exempt from the requirement. Additionally, financial institutions must report transaction on a Suspicious Activity Report (SAR) that they deem "suspicious", defined as a knowing or suspecting that the funds come from illegal activity or disguise funds from illegal activity, that it is structured to evade BSA requirements or appears to serve no known business or apparent lawful purpose; or that the institution is being used to facilitate criminal activity. Attempts by customers to circumvent the BSA, generally by structuring cash deposits to amounts lower than US$10,000 by breaking them up and depositing them on different days or at different locations also violates the law.

The financial database created by these reports is administered by the U.S.'s Financial Intelligence Unit (FIU), called the Financial Crimes Enforcement Network (FinCEN), located in Vienna, Virginia. The reports are made available to U.S. criminal investigators, as well as other FIU's around the globe, and FinCEN conducts computer assisted analyses of these reports to determine trends and refer investigations.

The BSA requires financial institutions to engage in customer due diligence, or KYC, which is sometimes known in the parlance as know your customer. This includes obtaining satisfactory identification to give assurance that the account is in the customer's true name, and having an understanding of the expected nature and source of the money that flows through the customer's accounts. Other classes of customers, such as those with private banking accounts and those of foreign government officials, are subjected to enhanced due diligence because the law deems that those types of accounts are a higher risk for money laundering. All accounts are subject to ongoing monitoring, in which internal bank software scrutinizes transactions and flags for manual inspection those that fall outside certain parameters. If a manual inspection reveals that the transaction is suspicious, the institution should file a Suspicious Activity Report.

The regulators of the industries involved are responsible to ensure that the financial institutions comply with the BSA. For example, the Federal Reserve and the Office of the Comptroller of the Currencyregularly inspect banks, and may impose civil fines or refer matters for criminal prosecution for non-compliance. A number of banks have been fined and prosecuted for failure to comply with the BSA. Most famously, Riggs Bank, in Washington D.C., was prosecuted and functionally driven out of business as

a result of its failure to apply proper money laundering controls, particularly as it related to foreign political figures.

In addition to the BSA, the U.S. imposes controls on the movement of currency across its borders, requiring individuals to report the transportation of cash in excess of US$10,000 on a form called Report of International Transportation of Currency or Monetary Instruments (known as a CMIR). Likewise, businesses, such as automobile dealerships, that receive cash in excess of US$10,000 must file a Form 8300 with the Internal Revenue Service, identifying the source of the cash.

On 1 September 2010, the Financial Crimes Enforcement Network issued an advisory on "informal value transfer systems" referencing *United States v. Banki*.

In the United States, there are perceived consequences of anti-money laundering (AML) regulations. These unintended consequences include FinCEN's publishing of a list of "risky businesses," which many believe unfairly targeted money service businesses. The publishing of this list and the subsequent fall-out, banks indiscriminately de-risking MSBs, is referred to as Operation Choke Point.

Criminal sanctions

Money laundering has been criminalized in the United States since the Money Laundering Control Act of 1986. The law, contained at section 1956 of Title 18 of the United States Code, prohibits individuals from engaging in a financial transaction with proceeds that were generated from certain specific crimes, known as "specified unlawful activities" (SUAs). The law requires that an individual specifically intend in making the transaction to conceal the source, ownership or control of the funds. There is no minimum threshold of money, and no requirement that the transaction succeeded in actually disguising the money. A "financial transaction" has been broadly defined, and need not involve a financial institution, or even a business. Merely passing money from one person to another, with the intent to disguise the source, ownership, location or control of the money, has been deemed a financial transaction under the law. The possession of money without either a financial transaction or an intent to conceal is not a crime in the United States. Besides money laundering, the law contained in section 1957 of Title 18 of the United States Code, prohibits spending more than US$10,000 derived from an SUA, regardless of whether the individual wishes to disguise it. It carries a lesser penalty than money laundering, and unlike the money laundering statute, requires that the money pass through a financial institution.

According to the records compiled by the United States Sentencing Commission, in 2009, the United States Department of Justice typically convicted a little over 81,000 people; of this, approximately 800 are convicted of money laundering as the primary or most serious charge. The Anti-Drug Abuse Act of 1988 expanded the definition of financial institution to include businesses such as car dealers and real estate closing personnel and required them to file reports on large currency transaction. It required verification of identity of those who purchase monetary instruments over $3,000. The Annunzio-Wylie Anti-Money Laundering Act of 1992 strengthened sanctions for BSA violations, required so called "Suspicious Activity Reports" and eliminated previously used "Criminal Referral Forms", required verification and recordkeeping for wire transfers and established the Bank Secrecy Act Advisory Group (BSAAG). The Money Laundering Suppression Act from 1994 required banking agencies to review and enhance training, develop anti-money laundering examination procedures, review and enhance procedures for referring cases to law enforcement agencies, streamlined the Currency transaction report exemption process, required each Money services business (MSB) to be registered by an owner or controlling person, required every MSB to maintain a list of businesses authorized to act as agents in connection with the financial services offered by the MSB, made operating an unregistered MSB a federal crime, and recommended that states adopt uniform laws applicable to MSBs. The Money Laundering and Financial Crimes Strategy Act of 1998 required banking agencies to develop anti-money laundering training for examiners, required the Department of the Treasury and other agencies to develop a "National Money Laundering Strategy", created the "High Intensity Money Laundering and Related Financial Crime Area" (HIFCA) Task Forces to concentrate law enforcement efforts at the federal, state and local levels in zones where money laundering is prevalent. HIFCA zones may be defined geographically or can be created to address money laundering in an industry sector, a financial institution, or group of financial institutions.

The Intelligence Reform & Terrorism Prevention Act of 2004 amended the Bank Secrecy Act to require the Secretary of the Treasury to prescribe regulations requiring certain financial institutions to report cross-border electronic transmittals of funds, if the Secretary determines that reporting is "reasonably necessary" in "anti-money laundering /combatting financing of terrorists (Anti-Money Laundering/Combating the Financing of Terrorism AML/CFT).

Notable cases

- Charter House Bank: Charter House Bank in Kenya was placed under statutory management in 2006 by the Central Bank of Kenya after it was discovered the bank was being used for money laundering activities by multiple accounts

containing missing customer information. More than $1.5 billion had been laundered before the scam was uncovered.Charter House Bank Kenya Scandal

- Bank of Credit and Commerce International: Unknown amount, estimated in billions, of criminal proceeds, including drug trafficking money, laundered during the mid-1980s.
- Bank of New York: US$7 billion of Russian capital flight laundered through accounts controlled by bank executives, late 1990s.
- Ferdinand Marcos: Unknown amount, estimated at US$10 billion of government assets laundered through banks and financial institutions in the United States, Liechtenstein, Austria, Panama, Netherlands Antilles, Cayman Islands, Vanuatu, Hong Kong, Singapore, Monaco, the Bahamas, the Vatican and Switzerland.
- HSBC, in December 2012, paid a record $1.9 Billion fines for money-laundering hundreds of millions of dollars for drug traffickers, terrorists and sanctioned governments such as Iran. The money-laundering occurred throughout the 2000s.
- Liberty Reserve, in May 2013, was seized by United States federal authorities for laundering $6 billion.
- Institute for the Works of Religion: Italian authorities investigated suspected money laundering transactions amounting to US$218 million made by the IOR to several Italian banks.
- Nauru: US$70 billion of Russian capital flight laundered through unregulated Nauru offshore shell banks, late 1990s
- Sani Abacha: US$2–5 billion of government assets laundered through banks in the UK, Luxembourg, Jersey (Channel Islands), and Switzerland, by the president of Nigeria.
- Standard Chartered: paid $330 million in fines for money-laundering hundreds of billions of dollars for Iran. The money-laundering took place in the 2000s and occurred for "nearly a decade to hide 60,000 transactions worth $250 billion".
- Standard Bank: Standard Bank South Africa London Branch – The Financial Conduct Authority (FCA) has fined Standard Bank PLC (Standard Bank) £7,640,400 for failings relating to its anti-money laundering (AML) policies and procedures over corporate and private bank customers connected to politically exposed persons (PEPs).
- BNP Paribas, in June 2014, pleaded guilty to falsifying business records and conspiracy, having violated U.S. sanctions against Cuba, Iran, and Sudan. It agreed to pay an $8.9 billion fine, the largest ever for violating U.S. sanctions.
- BSI Bank, in May 2017, was shut down by the Monetary Authority of Singapore for serious breaches of anti-money laundering requirements, poor

management oversight of the bank's operations, and gross misconduct of some of the bank's staff.

- Jose Franklin Jurado-Rodriguez, a Harvard College and Columbia University Graduate School of Arts and Sciences Economics Department alumnus, was convicted in Luxembourg in "June 1990 in what was one of the largest drug money laundering cases ever brought in Europe" and the US in 1996 of money laundering for the Cali Cartel kingpin Jose Santacruz Londono. Jurado-Rodriguez specialized in "smurfing".

Digital money

To prevent the usage of decentralized digital money such as Bitcoin for the profit of crime and corruption, Australia is planning to strengthen the nation's anti-money laundering laws. Knowing the characteristics of Bitcoin, it is completely deterministic, protocol based and cannot be censored, may circumvent national laws using services like Tor to obfuscate transaction origins, and relies completely off of cryptography, not a central entity running under a KYC framework. There are several cases of criminals have cashed out a significant amount of Bitcoin after ransomware attacks, drug dealings, cyber fraud and gunrunning. Other damages such as The DAO being drained of Ether cannot be classified as money laundering under any legal definition, as decentralized virtual environments are legally stateless and cannot be intervened with by a governing body. Such an incident has been debated as to the clear definition of money laundering in a stateless environment, leading to Ethereum Classic to form.

Fraud

In law, **fraud** is deliberate deception to secure unfair or unlawful gain, or to deprive a victim of a legal right. Fraud itself can be a civil wrong (i.e., a fraud victim may sue the fraud perpetrator to avoid the fraud or recover monetary compensation), a criminal wrong (i.e., a fraud perpetrator may be prosecuted and imprisoned by governmental authorities) or it may cause no loss of money, property or legal right but still be an element of another civil or criminal wrong. The purpose of fraud may be monetary gain or other benefits, such as obtaining a passport or travel document, driver's license or qualifying for a mortgageby way of false statements.

A hoax is a distinct concept that involves deliberate deception without the intention of gain or of materially damaging or depriving a victim.

In common law jurisdictions, as a civil wrong, fraud is a tort. While the precise definitions and requirements of proof vary among jurisdictions, the requisite elements of fraud as a tort generally are the intentional misrepresentation or concealment of an important fact upon which the victim is meant to rely, and in fact does rely, to the harm of the victim. Proving fraud in a court of law is often said to be difficult. That difficulty is found, for instance, in that each and every one of the elements of fraud must be proven, that the elements include proving the states of mind of the perpetrator and the victim, and that some jurisdictions require the victim to prove fraud by clear and convincing evidence.

The remedies for fraud may include rescission (i.e., reversal) of a fraudulently obtained agreement or transaction, the recovery of a monetary award to compensate for the harm caused, punitive damages to punish or deter the misconduct, and possibly others.

In cases of a fraudulently induced contract, fraud may serve as a defense in a civil action for breach of contract or specific performance of contract.

Fraud may serve as a basis for a court to invoke its equitable jurisdiction.

In common law jurisdictions, as a criminal offence, fraud takes many different forms, some general (e.g., theft by false pretense) and some specific to particular categories of victims or misconduct (e.g., bank fraud, insurance fraud, forgery). The elements of fraud as a crime similarly vary. The requisite elements of perhaps most general form of criminal fraud, theft by false pretense, are the intentional deception of a victim by false representation or pretense with the intent of persuading the victim to part with

property and with the victim parting with property in reliance on the representation or pretense and with the perpetrator intending to keep the property from the victim.

Section 380(1) of the Criminal Code provides the general definition for fraud in Canada:

380. (1) Every one who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security or any service,

> (a) is guilty of an indictable offence and liable to a term of imprisonment not exceeding fourteen years, where the subject-matter of the offence is a testamentary instrument or the value of the subject-matter of the offence exceeds five thousand dollars; or
> (b) is guilty
> (i) of an indictable offence and is liable to imprisonment for a term not exceeding two years, or
> (ii) of an offence punishable on summary conviction, where the value of the subject-matter of the offence does not exceed five thousand dollars.

In addition to the penalties outlined above, the court can also issue a prohibition order under s. 380.2 (preventing a person from "seeking, obtaining or continuing any employment, or becoming or being a volunteer in any capacity, that involves having authority over the real property, money or valuable security of another person"). It can also make a restitution order under s. 380.3.

The Canadian courts have held that the offence consists of two distinct elements:

- A prohibited act of deceit, falsehood or other fraudulent means. In the absence of deceit or falsehood, the courts will look objectively for a "dishonest act"; and
- The deprivation must be caused by the prohibited act, and deprivation must relate to property, money, valuable security, or any service.

The Supreme Court of Canada has held that deprivation is satisfied on proof of detriment, prejudice or risk of prejudice; it is not essential that there be actual loss. Deprivation of confidential information, in the nature of a trade secret or copyrighted material that has commercial value, has also been held to fall within the scope of the offence.

Zhang Yingyu's story collection The Book of Swindles (ca. 1617) testifies to rampant commercial fraud, especially involving itinerant businessmen, in late Ming China. The journal Science reported in 2017 that fraud is rife in Chinese academia, resulting in numerous article retractions and harm to China's international prestige. *The Economist*, CNN, and other media outlets regularly report on incidents of fraud or bad faith in Chinese business and trade practices. *Forbes* cites cybercrime as a persistent and growing threat to Chinese consumers.

"Half of all UK companies say that they have been the victim of fraud or of economic crime in the last two years [2016-2018], according to a major survey conducted by professional services firm PwC."

BBC News Online reported in 2016 that the estimated value lost through fraud in the UK was £193 billion a year.

In January 2018 the Financial Times reported that the value of UK fraud hit a 15-year high of £2.11bn in 2017 according to a study. The article said that the accountancy firm BDO examined reported fraud cases worth more than £50,000 and found that the total number rose to 577 in 2017, compared with 212 in 2003. The study found that the average amount stolen in each incident rose to £3.66m, up from £1.5m in 2003.

As at November 2017 Fraud is the most common criminal offence in the UK according to a study by Crowe Clark Whitehill, Experian and the Centre for Counter Fraud Studies. The study suggests the UK loses over £190 billion per year to fraud. £190 billion is more than 9% of the UK's projected GDP for 2017 ($2,496 (£2,080) billion according to Statistics Times). The estimate for fraud in the UK figure is more than the entire GDP of countries such as Romania, Qatar and Hungary.

According to another review by the UK anti-fraud charity Fraud Advisory Panel (FAP), business fraud accounted for £144bn, while fraud against individuals was estimated at £9.7bn. The FAP has been particularly critical of the support available from the police to victims of fraud in the UK outside of London. Although victims of fraud are generally referred to the UK's national fraud and cyber crime reporting centre, Action Fraud, the FAP found that there was "little chance" that these crime reports would be followed up with any kind of substantive law enforcement action by UK authorities, according to the report.

In July 2016 it was reported that fraudulent activity levels in the UK increased in the 10 years to 2016 from £52 billion to £193bn. This figure would be a conservative estimate, since as the former commissioner of the City of London Police, Adrian Leppard, has said, only 1 in 12 such crimes are actually reported. Donald Toon, director of the NCA's economic crime command, stated in July 2016: "The annual

losses to the UK from fraud are estimated to be more than £190bn". Figures released in October 2015 from the Crime Survey of England and Wales found that there had been 5.1 million incidents of fraud in England and Wales in the previous year, affecting an estimated one in 12 adults and making it the most common form of crime.

Also in July 2016, the Office for National Statistics (ONS) stated "Almost six million fraud and cyber crimes were committed last year in England and Wales and estimated there were two million computer misuse offences and 3.8 million fraud offences in the 12 months to the end of March 2016." Fraud affects one in ten people in the UK. According to the ONS most frauds relate to bank account fraud. These figures are separate from the headline estimate that another 6.3 million crimes (distinct from frauds) were perpetrated in the UK against adults in the year to March 2016.

Fraud is apparently low on the list UK law enforcement priorities. Controversially, the crime does not feature on a new "Crime Harm Index" published by the Office for National Statistics. Michael Levi, professor of criminology at Cardiff University, remarked in August 2016 that it was ‘deeply regrettable’ fraud is being left out of the first index despite being the most common crime reported to police in the UK. Professor Levi said ‘If you’ve got some categories that are excluded, they are automatically left out of the police’s priorities.’. The Chief of the National Audit Office (NAO), Sir Anyas Morse has also said “For too long, as a low-value but high-volume crime, online fraud has been overlooked by government, law enforcement and industry. It is now the most commonly experienced crime in England and Wales and demands an urgent response.”

The Fraud Act 2006 (c 35) is an Act of the Parliament of the United Kingdom. It affects England and Wales and Northern Ireland. It was given Royal Assenton 8 November 2006, and came into effect on 15 January 2007.

The Act gives a statutory definition of the criminal offence of fraud, defining it in three classes—fraud by false representation, fraud by failing to disclose information, and fraud by abuse of position. It provides that a person found guilty of fraud is liable to a fine or imprisonment for up to twelve months on summary conviction (six months in Northern Ireland), or a fine or imprisonment for up to ten years on conviction on indictment. This Act largely replaces the laws relating to obtaining property by deception, obtaining a pecuniary advantage and other offences that were created under the Theft Act 1978.

The Serious Fraud Office (United Kingdom) is an arm of the Government of the United Kingdom, accountable to the Attorney-General.

The National Fraud Authority (NFA) is the government agency co-ordinating the counter-fraud response in the UK.

Cifas is the UK's leading fraud prevention service, a not-for-profit membership organisation for all sectors that enables organisations to share and access fraud data using their databases. Cifas is dedicated to the prevention of fraud, including internal fraud by staff, and the identification of financial and related crime.

A Cifas study found that the number of reported cases of identity fraud jumped by 57 per cent between 2014 and 2015. Drawing from its reporting database of 261 organisations, Cifas found that 148,463 people reported having their identity stolen in 2015, up from 94,492 the previous year. The rise of social media has been blamed. Cifas has warned that social media sites such as Facebook, Twitter and LinkedIn are becoming a “hunting ground” for fraudsters.

In July 2016 the BBC referred to a recently published Cifas report which estimated the annual cost of fraud in the UK was £193bn – equal to nearly £3,000 per head of population.

In March 2017, Cifas reported that identity fraud had reached "record levels", with 173,000 cases recorded to its fraud database in 2016 – the highest number ever recorded by members of Cifas. That trend continued through 2017, with Cifas reporting more than 89,000 cases of identity fraud in the first six months of the year.

Cifas data from 2016 and 2017 also highlighted the growing issue of 'money mules' – people who allow their bank accounts to be used to launder money. Cifas reported that the number of young people (18-24-year-olds) allowing their accounts to be used to transfer the proceeds of crime had risen by an unprecedented 75 per cent in the last year.

The proof requirements for criminal fraud charges in the United States are essentially the same as the requirements for other crimes: guilt must be proved beyond a reasonable doubt. Throughout the United States fraud charges can be misdemeanors or felonies depending on the amount of loss involved. High value frauds can also include additional penalties. For example, in California losses of $500,000 or more will result in an extra two, three, or five years in prison in addition to the regular penalty for the fraud.

The U.S. government's 2006 fraud review concluded that fraud is a significantly under-reported crime, and while various agencies and organizations were attempting to tackle the issue, greater co-operation was needed to achieve a real impact in the

public sector. The scale of the problem pointed to the need for a small but high-powered body to bring together the numerous counter-fraud initiatives that existed.

According to Bloomberg, auto loan application fraud rates in the United States has been steadily rising over the past few years. This type of fraud expected to double from about $2-3 billion in 2015 to $4-6 billion in 2017.

Although elements may vary by jurisdiction and the specific allegations made by a plaintiff who files a lawsuit that alleged fraud, typical elements of a fraud case in the United States are that:

1. somebody misrepresents a material fact in order to obtain action or forbearance by another person,
2. the other person relies upon the misrepresentation, and
3. the other person suffers injury as a result of the act or forbearance taken in reliance upon the misrepresentation.

To establish a civil claim of fraud, most jurisdictions in the United States require that each element of a fraud claim be plead with particularity and be proved by a preponderance of the evidence, meaning that it is more likely than not that the fraud occurred. Some jurisdictions impose a higher evidentiary standard, such as Washington State's requirement that the elements of fraud be proved with clear, cogent, and convincing evidence (very probable evidence), or Pennsylvania's requirement that common law fraud be proved by clear and convincing evidence.

The measure of damages in fraud cases is normally computed using one of two rules:

1. the "benefit of bargain" rule, which allows for recovery of damages in the amount of the difference between the value of the property had it been as represented and its actual value; or
2. out-of-pocket loss, which allows for the recovery of damages in the amount of the difference between the value of what was given and the value of what was received.

Special damages may be allowed if shown to have been proximately caused by defendant's fraud and the damage amounts are proved with specificity.

Many jurisdictions permit a plaintiff in a fraud case to seek punitive or exemplary damages.

The typical organization loses five percent of its annual revenue to fraud, with a median loss of $160,000. Frauds committed by owners and executives were more than

nine times as costly as employee fraud. The industries most commonly affected are banking, manufacturing, and government.

Fraud can be committed through many media, including mail, wire, phone, and the Internet (computer crime and Internet fraud). International dimensions of the web and ease with which users can hide their location, the difficulty of checking identity and legitimacy online, and the simplicity with which hackers can divert browsers to dishonest sites and steal credit card details have all contributed to the very rapid growth of Internet fraud. In some countries, tax fraud is also prosecuted under false billing or tax forgery. There have also been fraudulent "discoveries", e.g., in science, to gain prestige rather than immediate monetary gain.

Beyond laws that aim at prevention of fraud, there are also governmental and non-governmental organizations that aim to fight fraud. Between 1911 and 1933, 47 states adopted the so-called Blue Sky Lawsstatus. These laws were enacted and enforced at the state level and regulated the offering and sale of securities to protect the public from fraud. Though the specific provisions of these laws varied among states, they all required the registration of all securities offerings and sales, as well as of every U.S. stockbroker and brokerage firm. However, these Blue Sky laws were generally found to be ineffective. To increase public trust in the capital markets the President of the United States, Franklin D. Roosevelt, established the U.S. Securities and Exchange Commission (SEC). The main reason for the creation of the SEC was to regulate the stock market and prevent corporate abuses relating to the offering and sale of securities and corporate reporting. The SEC was given the power to license and regulate stock exchanges, the companies whose securities traded on them, and the brokers and dealers who conducted the trading.

For detection of fraudulent activities on the large scale, massive use of (online) data analysis is required, in particular predictive analytics or forensic analytics. Forensic analytics is the use of electronic data to reconstruct or detect financial fraud. The steps in the process are data collection, data preparation, data analysis, and the preparation of a report and possibly a presentation of the results. Using computer-based analytic methods Nigrini's wider goal is the detection of fraud, errors, anomalies, inefficiencies, and biases which refer to people gravitating to certain dollar amounts to get past internal control thresholds.

The analytic tests usually start with high-level data overview tests to spot highly significant irregularities. In a recent purchasing card application these tests identified a purchasing card transaction for 3,000,000 Costa Rica Colons. This was neither a fraud nor an error, but it was a highly unusual amount for a purchasing card transaction. These high-level tests include tests related to Benford's Law and possibly also those statistics known as descriptive statistics. These high-tests are always

followed by more focused tests to look for small samples of highly irregular transactions. The familiar methods of correlation and time-series analysis can also be used to detect fraud and other irregularities. Forensic analytics also includes the use of a fraud risk-scoring model to identify high risk forensic units (customers, employees, locations, insurance claims and so on). Forensic analytics also includes suggested tests to identify financial statement irregularities, but the general rule is that analytic methods alone are not too successful at detecting financial statement fraud.

Notable fraudsters

- Alfredo Sáenz Abad, lied about bank loans as a banker so that some customers to the bank went to prison; he was later sentenced to prison, but managed to get a pardon and kept his job
- Frank Abagnale Jr., American impostor who wrote bad checks and falsely represented himself as a qualified member of professions such as airline pilot, doctor, attorney, and teacher; the film *Catch Me If You Can* is based on his life
- John Bodkin Adams, British doctor and suspected serial killer, but only found guilty of forging wills and prescriptions
- Eddie Antar, founder of Crazy Eddie; has criminal convictions on 17 counts and about $1 billion worth of civil judgments against him stemming from fraudulent accounting practices at that company
- Jordan Belfort, "The Wolf of Wall Street"; swindled over $200 million via a penny stock boiler room operation; the film "The Wolf of Wall Street" starring Leonardo DiCaprio is based on his life and fraudulent activity
- Cassie Chadwick, pretended to be Andrew Carnegie's illegitimate daughter to get loans
- Columbia/HCA Medicare fraud; Columbia/HCA pleaded guilty to 14 felony counts and paid out more than $2 billion to settle lawsuits arising from the fraudThe company's board of directors forced then–Chairman and CEO Rick Scott to resign at the beginning of the federal investigation; Scott was subsequently elected Governor of Florida in 2010
- Edward Davenport, self-styled "Lord"; nicknamed "Fast Eddie"and "Lord of Fraud";from 2005 to 2009 was the "ringmaster" of a series of advance-fee fraud schemes that defrauded dozens of individuals out of millions of pounds; is said to have made £34.5 million through various frauds
- Marc Dreier, managing founder of attorney firm Dreir LLP, a $700 million Ponzi scheme
- Enric Durán, defrauded Spanish banks and then gave away the loaned money to anti-growth organizations
- Bernard Ebbers, founder of WorldCom, which inflated its asset statements by about $11 billion

- Ramón Báez Figueroa, banker from the Dominican Republic and former President of Banco Intercontinental; sentenced in 2007 to 10 years in prison for a U.S. $2.2 billion fraud case that drove the Caribbean nation into economic crisis in 2003
- Martin Frankel, American former financier, convicted in 2002 of insurance fraud worth $208 million, racketeering and money laundering
- Samuel Israel III, former hedge fund manager; ran the former fraudulent Bayou Hedge Fund Group; faked suicide to avoid jail
- Konrad Kujau, German fraudster and forger responsible for the "Hitler Diaries"
- Kenneth Lay, American businessman who built energy company Enron; one of the highest paid CEOs in the U.S. until he was ousted as chairman and convicted of fraud and conspiracy, although, as a result of his death, his conviction was vacated
- Nick Leeson, English trader whose unsupervised speculative trading caused the collapse of Barings Bank
- James Paul Lewis, Jr., ran one of the biggest ($311 million) and longest running Ponzi schemes (20 years) in U.S. history
- Gregor MacGregor, Scottish con man; tried to attract investment and settlers for the non-existent country of Poyais
- Bernard Madoff, creator of a $65 billion Ponzi scheme, the largest investor fraud ever attributed to a single individual
- Matt the Knife, American con artist, card cheat and pickpocket; from age approximately 14 through 21, bilked dozens of casinos, corporations and at least one Mafia crime family out of untold sums
- Gaston Means, professional con man during U.S. President Warren G. Harding's administration
- Barry Minkow, ZZZZ Best scam
- Michael Monus, founder of Phar-Mor, which ultimately cost its investors more than $1 billion
- F. Bam Morrison, conned the town of Wetumka, Oklahoma by promoting a circus that never came
- Lou Pearlman, former boy-band manager and operator of a $300 million Ponzi scheme using two shell companies
- Frederick Emerson Peters, American impersonator who wrote bad checks
- Thomas Petters, American masquerading as a business manwho turned out to be a con man; former CEO and chairman of Petters Group Worldwide; resigned his position as CEO in 2008 amid mounting criminal investigations; later convicted for turning Petters Group Worldwide into a $3.65 billion Ponzi scheme; sentenced to 50 years in federal prison
- Charles Ponzi, Ponzi scheme
- Gert Postel, German mailman; worked as a psychiatrist in different hospitals

- Alves Reis, forged documents to print 100,000,000 PTE in official escudo banknotes (adjusted for inflation, it would be worth about US$150 million today)
- John Rigas, cable television entrepreneur, co-founder of Adelphia Communications Corporation and owner of the Buffalo Sabres hockey team; defrauded investors of over $2 billion and was sentenced to a 12-year term in federal prison
- Christopher Rocancourt, a Rockefeller impersonator who defrauded Hollywood celebrities
- Scott W. Rothstein, disbarred lawyer from Ft. Lauderdale, Florida; perpetrated a Ponzi scheme which defrauded investors of over $1 billion
- Michael Sabo, best known as a check, stocks and bonds forger; became notorious in the 1960s throughout the 1990s as a "Great Impostor" with over 100 aliases, and earned millions from such
- John Spano, struggling businessman who faked massive success in an attempt to buy out the New York Islanders of the NHL
- Allen Stanford, self-styled banker; sold fake certificates of deposit to people in many countries, raking in $7 billion to $8 billion over decades
- John Stonehouse, the last Postmaster-General of the UK and MP; faked his death to marry his mistress
- Kevin Trudeau, American writer and billiards promoter; convicted of fraud and larceny in 1991; known for a series of late-night infomercials and his series of books about "Natural Cures 'They' Don't Want You to Know About"
- Richard Whitney, stole from the New York Stock Exchange Gratuity Fund in the 1930s

Credit card fraud

Credit card fraud is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account. Credit card fraud is also an adjunct to identity theft. According to the United States Federal Trade Commission, while the rate of identity theft had been holding steady during the mid 2000s, it increased by 21 percent in 2008. However, credit card fraud, that crime which most people associate with ID theft, decreased as a percentage of all ID theft complaints for the sixth year in a row.

Although incidences of credit card fraud are limited to about 0.1% of all card transactions, they have resulted in huge financial losses as the fraudulent transactions have been large value transactions. In 1999, out of 12 billion transactions made annually, approximately 10 million—or one out of every 1200 transactions—turned out to be fraudulent. Also, 0.04% (4 out of every 10,000) of all monthly active accounts were fraudulent. Even with tremendous volume and value increase in credit card transactions since then, these proportions have stayed the same or have decreased due to sophisticated fraud detection and prevention systems. Today's fraud detection systems are designed to prevent one-twelfth of one percent of all transactions processed which still translates into billions of dollars in losses.

In the decade to 2008, general credit card losses have been 7 basis points or lower (i.e. losses of $0.07 or less per $100 of transactions). In 2007, fraud in the United Kingdom was estimated at £535 million.

Card fraud begins either with the theft of the physical card or with the compromise of data associated with the account, including the card account number or other information that would routinely and necessarily be available to a merchant during a legitimate transaction. The compromise can occur by many common routes and can usually be conducted without tipping off the cardholder, the merchant, or the issuer at least until the account is ultimately used for fraud. A simple example is that of a store clerk copying sales receipts for later use. The rapid growth of credit card use on the Internet has made database security lapses particularly costly; in some cases, millions of accounts have been compromised.

Stolen cards can be reported quickly by cardholders, but a compromised account can be hoarded by a thief for weeks or months before any fraudulent use, making it difficult to identify the source of the compromise. The cardholder may not discover fraudulent use until receiving a billing statement, which may be delivered

infrequently. Cardholders can mitigate this fraud risk by checking their account frequently to ensure constant awareness in case there are any suspicious, unknown transactions or activities.

When a credit card is lost or stolen, it may be used for illegal purchases until the holder notifies the issuing bank and the bank puts a block on the account. Most banks have free 24-hour telephone numbers to encourage prompt reporting. Still, it is possible for a thief to make unauthorized purchases on a card before the card is canceled. Without other security measures, a thief could potentially purchase thousands of dollars in merchandise or services before the cardholder or the card issuer realizes that the card has been compromised.

The only common security measure on all cards is a signature panel, but, depending on its exact design, a signature may be relatively easy to forge. Some merchants will demand to see a picture ID, such as a driver's license, to verify the identity of the purchaser, and some credit cards include the holder's picture on the card itself. In some jurisdictions, it is illegal for merchants to demand cardholder identification. Self-serve payment systems (gas stations, kiosks, etc.) are common targets for stolen cards, as there is no way to verify the card holder's identity. There is also a new law that has been implemented that identification or a signature is only required for purchases above $50 unless stated in the policy of the merchant. This new law makes it easier for credit card theft to take place as well because it is not making it necessary for a form of identification to be presented, so as long as the fraud is done at what is considered to be a small amount, little to no action is taken by the merchant to prevent it.

A common countermeasure is to require the user to key in some identifying information, such as the user's ZIP or postal code. This method may deter casual theft of a card found alone, but if the card holder's wallet is stolen, it may be trivial for the thief to deduce the information by looking at other items in the wallet. For instance, a U.S. driver license commonly has the holder's home address and ZIP code printed on it. Visa Inc. offers merchants lower rates on transactions if the customer provides a ZIP code.

In Europe, most cards are equipped with an EMV chip which requires a 4 to 6 digit PIN to be entered into the merchant's terminal before payment will be authorized. However, a PIN isn't required for online transactions and is often not required for transactions using the magnetic strip. However magnetic strip transactions are banned under the EMV system (which requires the PIN). In many/most European countries, if you don't have a card with a chip, you will usually be asked for photo-ID - e.g. national ID card, passport, etc. at the point of sale. Many self-service machines (e.g.

ticket machines at railway stations, and self-service check-in at airports) require a PIN and chip in EMV-land (i.e. which is most of Europe, Asia, Middle East etc.).

Requiring a customer's ZIP code is illegal in California, where the state's 1971 law prohibits merchants from requesting or requiring a cardholder's "personal identification information" as a condition of accepting the card for payment. The California Supreme Court has ruled that the ZIP code qualifies as personal identification information because it is part of the cardholder's address. Companies face fines of $250–1000 for each violation. Requiring a "personal identification number" (PIN) may also be a violation.

Card issuers have several countermeasures, including sophisticated software that can, prior to an authorized transaction, estimate the probability of fraud. For example, a large transaction occurring a great distance from the cardholder's home might seem suspicious. The merchant may be instructed to call the card issuer for verification or to decline the transaction, or even to hold the card and refuse to return it to the customer. The customer must contact the issuer and prove who they are to get their card back (if it is not fraud and they are actually buying a product).

In some countries, a credit card holder can make a contactless payment for goods or services by tapping their credit (or debit) card against a RFID or NFC reader without the need for a PIN or signature if the total price falls under a pre-determined floor limit (for example, in Australia this limit is currently at 100 AUD). A stolen credit or debit card could be used for a significant amount of these transactions before the true owner can have the account canceled.

Card information is stored in a number of formats. Card numbers – formally the Primary Account Number (PAN) – are often embossed or imprinted on the card, and a magnetic stripe on the back contains the data in machine-readable format. Fields can vary, but the most common include:

- Name of card holder
- Card number
- Expiration date
- Verification/CVV code
- The mail and the Internet are major routes for fraud against merchants who sell and ship products and affect legitimate mail-order and Internet merchants. If the card is not physically present (called CNP, card not present) the merchant must rely on the holder (or someone purporting to be so) presenting the information indirectly, whether by mail, telephone or over the Internet. The credit card holder can be tracked by mail or phone. While there are safeguards

to this, it is still more risky than presenting in person, and indeed card issuers tend to charge a greater transaction rate for CNP, because of the greater risk.

- It is difficult for a merchant to verify that the actual cardholder is indeed authorizing the purchase. Shipping companies can guarantee delivery to a location, but they are not required to check identification and they are usually not involved in processing payments for the merchandise. A common recent preventive measure for merchants is to allow shipment only to an address approved by the cardholder, and merchant banking systems offer simple methods of verifying this information. Before this and similar countermeasures were introduced, mail order carding was rampant as early as 1992. A *carder* would obtain the credit card information for a local resident and then intercept the delivery of the illegitimately purchased merchandise at the shipping address, often by staking out the porch of the residence.
- Small transactions generally undergo less scrutiny and are less likely to be investigated by either the card issuer or the merchant. CNP merchants must take extra precaution against fraud exposure and associated losses, and they pay higher rates for the privilege of accepting cards. Fraudsters bet on the fact that many fraud prevention features are not used for small transactions.
- Merchant associations have developed some prevention measures, such as single-use card numbers, but these have not met with much success. Customers expect to be able to use their credit card without any hassles and have little incentive to pursue additional security due to laws limiting customer liability in the event of fraud. Merchants can implement these prevention measures but risk losing business if the customer chooses not to use them.

Identity theft can be divided into two broad categories: application fraud and account takeover.

Application fraud takes place when a person uses stolen or fake documents to open an account in another person's name. Criminals may steal documents such as utility bills and bank statements to build up useful personal information. Alternatively, they may create fake documents. With this information, they could open a credit card account or Ioan account in the victim's name, and then fully draw it.

An account takeover occurs when criminals pose as a genuine customer, gain control of an account and then makes unauthorized transactions. According to Action Fraud, fraud is committed at the point money is lost. An account takeover refers to the act by which fraudsters will attempt to assume control of a customer’s account from a broad array of service providers such as credit cards, email, banks, and more. Control at the account level offers better long-term returns for fraudsters but can be extremely

harmful to the rightful account owners. According to Forrester, risk-based authentication (RBA) plays a key role in identity and access management (IAM) and risk mitigation of account takeover attacks that result in up to $7 billion in annual losses.

The most prominent types of account takeovers deal with credit card fraud. As opposed to stealing credit card numbers which can be changed after the user reports it lost or stolen, fraudsters prefer account takeover to maximize their return on investment. A fraudster uses parts of the victim’s identity such as an email address to gain access to financial accounts. This individual then intercepts communication about the account to keep the victim blind to any threats. Victims are often the first to detect account takeover when they discover charges on monthly statements they did not authorize or multiple questionable withdrawals. Recently there has been an increase in the number of account takeovers since the adoption of EMV technology, which makes it more difficult for fraudsters to clone physical credit cards.

Among some of the most common methods by which a fraudster will commit an account takeover include brute force botnet attacks, phishing, and malware. Other methods include dumpster diving to find personal information in discarded mail, and outright buying lists of 'Fullz,' a slang term for full packages of identifying information sold on the black market.

"Skimmer (device)" redirects here. For other uses, see Skimmer (disambiguation).

Skimming is the crime of getting private information about somebody else's credit card used in an otherwise normal transaction. The thief can procure a victim's card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store hundreds of victims' card numbers. Common scenarios for skimming are restaurants or bars where the skimmer has possession of the victim's payment card out of their immediate view. The thief may also use a small keypad to unobtrusively transcribe the 3 or 4 digit card security code, which is not present on the magnetic strip. Call centers are another area where skimming can easily occur. Skimming can also occur at merchants such as gas stations when a third-party card-reading device is installed either outside or inside a fuel dispenser or other card-swiping terminal. This device allows a thief to capture a customer's card information, including their PIN, with each card swipe.

Instances of skimming have been reported where the perpetrator has put over the card slot of an ATM (automated teller machine) a device that reads the magnetic strip as the user unknowingly passes their card through it. These devices are often used in conjunction with a miniature camera (inconspicuously attached to the ATM) to read

the user's PIN at the same time. This method is being used in many parts of the world, including South America, Argentina, and Europe. Another technique used is a keypad overlay that matches up with the buttons of the legitimate keypad below it and presses them when operated, but records or wirelessly transmits the keylog of the PIN entered. The device or group of devices illicitly installed on an ATM are also colloquially known as a "skimmer". Recently made ATMs now often run a picture of what the slot and keypad are supposed to look like as a background so that consumers can identify foreign devices attached.

Skimming is difficult for the typical cardholder to detect, but given a large enough sample, it is fairly easy for the card issuer to detect. The issuer collects a list of all the cardholders who have complained about fraudulent transactions, and then uses data mining to discover relationships among them and the merchants they use. For example, if many of the cardholders use a particular merchant, that merchant can be directly investigated. Sophisticated algorithms can also search for patterns of fraud. Merchants must ensure the physical security of their terminals, and penalties for merchants can be severe if they are compromised, ranging from large fines by the issuer to complete exclusion from the system, which can be a death blow to businesses such as restaurants where credit card transactions are the norm.

Checker is a term used for a process to verify the validity of stolen card data. The thief presents the card information on a website that has real-time transaction processing. If the card is processed successfully, the thief knows that the card is still good. The specific item purchased is immaterial, and the thief does not need to purchase an actual product; a website subscription or charitable donation would be sufficient. The purchase is usually for a small monetary amount, both to avoid using the card's credit limit, and also to avoid attracting the card issuer's attention. A website known to be susceptible to carding is known as a cardable website.

In the past, carders used computer programs called "generators" to produce a sequence of credit card numbers, and then test them to see which were valid accounts. Another variation would be to take false card numbers to a location that does not immediately process card numbers, such as a trade show or special event. However, this process is no longer viable due to widespread requirement by internet credit card processing systems for additional data such as the billing address, the 3 to 4 digit Card Security Code and/or the card's expiration date, as well as the more prevalent use of wireless card scanners that can process transactions right away. Nowadays, carding is more typically used to verify credit card data obtained directly from the victims by skimming or phishing.

A set of credit card details that have been verified in this way is known in fraud circles as a phish. A carder will typically sell data files of the phish to other

individuals who will carry out the actual fraud. The market price for a phish ranges from US$1.00 to US$50.00 depending on the type of card, the freshness of the data and credit status of the victim.

Credit cards are produced in BIN ranges. Where an issuer does not use random generation of the card number, it is possible for an attacker to obtain one good card number and generate valid card numbers. But the probability for such an action remains very low and because of the presence of the Valid date / Expire date and the CVV.

Scammers may use a variety of schemes to lure victims into giving them their card information through tricks such as websites pretending to be of a bank or payment system. Telephone phishing can also be employed, in which a call center is set up to pretend to be associated with a banking organization.

Some promotional offers include active balance transfer checks which may be tied directly to a credit card account. These are often sent unsolicited and may occur as often as once per month by some financial institutions. In cases where checks are stolen from a victim's mailbox, they can be used at a point of sales location thereby leaving the victim responsible for the losses. They are one path at times used by fraudsters.

When a cardholder buys something from a vendor and expects the card to be charged only once, a vendor may charge the card a small amount multiple times at infrequent intervals such as monthly or annually until the card expires. The vendor may state in the fine print that the customer is now a "member" and the membership will be renewed periodically unless the cardholder notifies the vendor in accordance with a cancellation procedure in the "membership agreement" which the cardholder agreed to when they made the initial purchase. Because the periodic charges are unexpected, infrequent, and small, most cardholders will not notice the charges. If a cardholder complains to the bank that the charges were unauthorized, the bank will notify the vendor of the disputed charges and the vendor will respond that the cardholder never canceled the "membership" which the cardholder agreed to. Since most card holders have no idea what the cancellation procedure is and the vendor will reveal it only to new customers, the bank will not reverse the charges, but instead will offer to cancel the credit card and reissue it with a different account number or expiration date. Unexpected repeat billing is in a gray area of the law, depending on whether the customer legitimately agreed to the charges.

Online bill paying or internet purchases utilizing a bank account are a source for repeat billing known as "recurring bank charges". These are standing orders or banker's orders from a customer to honor and pay a certain amount every month to the

payee. With E-commerce, especially in the United States, a vendor or payee can receive payment by direct debit through an Automated Clearing House (ACH). While many payments or purchases are valid, and the customer has intentions to pay the bill monthly, some are known as *Rogue Automatic Payments*.

Another type of credit card fraud targets utility customers. Customers receive unsolicited in-person, telephone, or electronic communication from individuals claiming to be representatives of utility companies. The scammers alert customers that their utilities will be disconnected unless an immediate payment is made, usually involving the use of a reloadable debit card to receive payment. Sometimes the scammers use authentic-looking phone numbers and graphics to deceive victims. The Edison Electric Institute (EEI) and a coalition of electric, gas and water companies from across North America created the Utilities United Against Scams Day beginning November 16, 2016, to raise awareness about scams that target utility customers.

The Department of Justice has announced in September 2014 that it will seek to impose a tougher law to combat overseas credit card trafficking. Authorities say the current statute is too weak because it allows people in other countries to avoid prosecution if they stay outside the United States when buying and selling the data and don't pass their illicit business through the U.S. The Department of Justice asks Congress to amend the current law that would make it illegal for an international criminal to possess, buy or sell a stolen credit card issued by a U.S. bank independent of geographic location.

In the US, federal law limits the liability of card holders to $50 in the event of theft of the actual credit card, regardless of the amount charged on the card, if reported within 60 days of receiving the statement. In practice many issuers will waive this small payment and simply remove the fraudulent charges from the customer's account if the customer signs an affidavit confirming that the charges are indeed fraudulent. If the physical card is not lost or stolen, but rather just the credit card account number itself is stolen, then Federal Law guarantees cardholders have zero liability to the credit card issuer.

The merchants and the financial institutions bear the loss. The merchant loses the value of any goods or services sold and any associated fees. If the financial institution does not have a charge-back right then the financial institution bears the loss and the merchant does not suffer at all. These losses incline merchants to be cautious and often they ban legitimate transactions and lose potential revenues. Online merchants can choose to apply for additional services that credit card companies offer, such as Verified by Visa and MasterCard SecureCode. However, these are complicated and

awkward to do or use for consumers so there is a trade-off between making a sale easy and making it secure.

The liability for the fraud is determined by the details of the transaction. If the merchant retrieved all the necessary pieces of information and followed all of the rules and regulations the financial institution would bear the liability for the fraud. If the merchant did not get all of the necessary information they would be required to return the funds to the financial institution. This is all determined by the credit card processors.

In the UK, credit cards are regulated by the Consumer Credit Act 1974 (amended 2006). This provides a number of protections and requirements.

Any misuse of the card, unless deliberately criminal on the part of the cardholder, must be refunded by the merchant or card issuer.

In Australia, credit card fraud is considered a form of 'identity crime'. The Australian Transaction Reports and Analysis Centre has established standard definitions in relation to identity crime for use by law enforcement across Australia:

- The term **identity** encompasses the identity of natural persons (living or deceased) and the identity of bodies corporate
- **Identity fabrication** describes the creation of a fictitious identity
- **Identity manipulation** describes the alteration of one's own identity
- **Identity theft** describes the theft or assumption of a pre-existing identity (or significant part thereof), with or without consent and whether, in the case of an individual, the person is living or deceased
- **Identity crime** is a generic term to describe activities/offences in which a perpetrator uses a fabricated identity, a manipulated identity, or a stolen/assumed identity to facilitate the commission of a crime(s).

Estimates created by the Attorney-General's Department show that identity crime costs Australia upwards of $1.6 billion each year, with majority of about $900 million being lost by individuals through credit card fraud, identity theft and scams. In 2015, the Minister for Justice and Minister Assisting the Prime Minister for Counter-Terrorism, Michael Keenan, released the report Identity Crime and Misuse in Australia 2013-14. This report estimated that the total direct and indirect cost of identity crime was closer to $2 billion, which includes the direct and indirect losses experienced by government agencies and individuals, and the cost of identity crimes recorded by police.

The victim of credit card fraud in Australia, still in possession of the card, is not responsible for anything bought on it without their permission. However, this is subject to the terms and conditions of the account. If the card has been reported physically stolen or lost the cardholder is usually not responsible for any transactions not made by them, unless it can be shown that the cardholder acted dishonestly or without reasonable care.

In Sweden, the card issuer shall compensate the cardholder for fraudulent usage. The exception is if the cardholder handled the card in a careless way, which can include leaving a handbag with the card out of sight in a public place. Then the cardholder must take the loss, normally limited to 12000 SEK (1402 USD), but unlimited in case of serious carelessness. Credit card purchases are normally verified by a PIN code or identity card in Sweden. If such a check was not performed (which is normal for internet purchases) the merchant must take the loss.

To prevent being "charged back" for fraud transactions, merchants can sign up for services offered by Visa and MasterCard called Verified by Visa and MasterCard SecureCode, under the umbrella term 3-D Secure. This requires consumers to add additional information to confirm a transaction.

Often enough online merchants do not take adequate measures to protect their websites from fraud attacks, for example by being blind to sequencing. In contrast to more automated product transactions, a clerk overseeing "card present" authorization requests must approve the customer's removal of the goods from the premises in real time.

Credit card merchant associations, like Visa and MasterCard, receive profits from transaction fees, charging between 0% and 3.25% of the purchase price plus a per transaction fee of between 0.00 USD and 40.00 USD. Cash costs more to bank up, so it is worthwhile for merchants to take cards. Issuers are thus motivated to pursue policies which increase the money transferred by their systems. Many merchants believe this pursuit of revenue reduces the incentive for credit card issuers to adopt procedures to reduce crime, particularly because the cost of investigating a fraud is usually higher than the cost of just writing it off. These costs are passed on to the merchants as "chargebacks". This can result in substantial additional costs: not only has the merchant been defrauded for the amount of the transaction, he is also obliged to pay the chargeback fee, and to add insult to injury the transaction fees still stand. Additionally, merchants may lose their merchant account if their percent of chargeback to overall turnover exceeds some value related to their type of product or service sold.

Merchants have started to request changes in state and federal laws to protect themselves and their consumers from fraud, but the credit card industry has opposed many of the requests. In many cases, merchants have little ability to fight fraud, and must simply accept a proportion of fraud as a cost of doing business.

Because all card-accepting merchants and card-carrying customers are bound by civil contract law there are few criminal laws covering the fraud. Payment transfer associations enact changes to regulations, and the three parties— the issuer, the consumer, and the merchant— are all generally bound to the conditions, by a self-acceptance term in the contract that it can be changed.

The merchant loses the payment, the fees for processing the payment, any currency conversion commissions, and the amount of the chargeback penalty. For obvious reasons, many merchants take steps to avoid chargebacks—such as not accepting suspicious transactions. This may spawn collateral damage, where the merchant additionally loses legitimate sales by incorrectly blocking legitimate transactions. Mail Order/Telephone Order (MOTO) merchants are implementing Agent-assisted automation which allows the call center agent to collect the credit card number and other personally identifiable informationwithout ever seeing or hearing it. This greatly reduces the probability of chargebacks and increases the likelihood that fraudulent chargebacks will be successfully overturned.

Between July 2005 and mid-January 2007, a breach of systems at TJX Companies exposed data from more than 45.6 million credit cards. Albert Gonzalez is accused of being the ringleader of the group responsible for the thefts. In August 2009 Gonzalez was also indicted for the biggest known credit card theft to date — information from more than 130 million credit and debit cards was stolen at Heartland Payment Systems, retailers 7-Eleven and Hannaford Brothers, and two unidentified companies.

In 2012, about 40 million sets of payment card information were compromised by a hack of Adobe Systems. The information compromised included customer names, encrypted payment card numbers, expiration dates and information relating to orders Chief Security Officer Brad Arkin said.

In July 2013, press reports indicated four Russians and a Ukrainian were indicted in the U.S. state of New Jersey for what was called “the largest hacking and data breach scheme ever prosecuted in the United States.” Albert Gonzalez was also cited as a co-conspirator of the attack, which saw at least 160 million credit card losses and excess of $300 million in losses. The attack affected both American and European companies including Citigroup, Nasdaq OMX Group, PNC Financial Services Group, Visa licensee Visa Jordan, Carrefour, J. C. Penny and JetBlue Airways.

Between 27 November 2013 and 15 December 2013 a breach of systems at Target Corporation exposed data from about 40 million credit cards. The information stolen included names, account number, expiry date and Card security code.

From 16 July to 30 October 2013, a hacking attack compromised about a million sets of payment card data stored on computers at Neiman-Marcus. A malware system, designed to hook into cash registers and monitor the credit card authorisation process (RAM-scraping malware), infiltrated Target's systems and exposed information from as many as 110 million customers.

On September 8, 2014, The Home Depot confirmed that their payment systems were compromised. They later released a statement saying that the hackers obtained a total of 56 million credit card numbers as a result of the breach.

On May 15, 2016, in a coordinated attack, a group of around 100 individuals used the data of 1600 South African credit cards to steal 12.7 million USD from 1400 convenience stores in Tokyo within three hours. Using a Sunday and acting in another country than the bank which issued the cards, they are believed to have won enough time to leave Japan before the heist was discovered.

Countermeasures to combat credit card fraud include the following.

By merchants:

- PAN truncation – not displaying the full number on receipts
- Tokenization (data security) – not storing the full number in computer systems
- Requesting additional information, such as a PIN, ZIP code, or Card Security Code
- Perform geolocation validation, such as IP address
- Use of Reliance Authentication, indirectly via PayPal, or directly via iSignthis or miiCard.

By card issuers:

- Fraud detection and prevention software that analyzes patterns of normal and unusual behavior as well as individual transactions in order to flag likely fraud. Profiles include such information as IP address. Technologies have existed since the early 1990s to detect potential fraud. One early market entrant was Falcon; other leading software solutions for card fraud include Actimize, SAS, BAE Systems Detica, and IBM.
- Fraud detection and response business processes such as:
    - Contacting the cardholder to request verification

    - Placing preventative controls/holds on accounts which may have been victimized
    - Blocking card until transactions are verified by cardholder
    - Investigating fraudulent activity
- Strong Authentication measures such as:
    - Multi-factor Authentication, verifying that the account is being accessed by the cardholder through requirement of additional information such as account number, PIN, ZIP, challenge questions
    - Multi possession-factor authentication, verifying that the account is being accessed by the cardholder through requirement of additional personal devices such as smart watch, smart phone Challenge-response authentication
    - Out-of-band Authentication, verifying that the transaction is being done by the cardholder through a "known" or "trusted" communication channel such as text message, phone call, or security token device
- Industry collaboration and information sharing about known fraudsters and emerging threat vectors

By Governmental and Regulatory Bodies:

- Enacting consumer protection laws related to card fraud
- Performing regular examinations and risk assessments of credit card issuers
- Publishing standards, guidance, and guidelines for protecting cardholder information and monitoring for fraudulent activity
- Regulation, such as that introduced in the SEPA and EU28 by the European Central Bank's 'SecuRe Pay' requirements and the Payment Services Directive 2 legislation.

By cardholders:

- Reporting lost or stolen cards
- Reviewing charges regularly and reporting unauthorized transactions immediately
- Installing virus protection software on personal computers
- Using caution when using credit cards for online purchases, especially on non-trusted websites
- Keeping a record of account numbers, their expiration dates, and the phone number and address of each company in a secure place.

Additional technological features:

- 3-D Secure

- EMV
- Point to Point Encryption
- Strong authentication
- True Link

Cheque fraud

Cheque fraud refers to a category of criminal acts that involve making the unlawful use of cheques in order to illegally acquire or borrow funds that do not exist within the account balance or account-holder's legal ownership. Most methods involve taking advantage of the *float* (the time between the negotiation of the cheque and its clearance at the cheque-writer's bank) to draw out these funds. Specific kinds of cheque fraud include **cheque kiting**, where funds are deposited before the end of the float period to cover the fraud, and **paper hanging**, where the float offers the opportunity to write fraudulent cheques but the account is never replenished.

Cheque kiting refers to use of the float to take advantage and delay the notice of non-existent funds.

While some cheque kiters fully intend to bring their accounts into good standing, others, often known as *paper hangers*, have pure fraud in mind, attempting to "take the money and run."

A cheque is written to a merchant or other recipient, hoping the recipient will not suspect that the cheque will not clear. The buyer will then take possession of the cash, goods, or services purchased with the cheque, and will hope the recipient will not take action or will do so in vain.

The paper hanger deposits a cheque one time that s/he knows is bad or fictitious into his/her account. When the bank considers the funds available (usually on the next business day), but before the bank is informed the cheque is bad, the paper hanger then withdraws the funds in cash. The offender knows the cheque will bounce, and the resulting account will be in debt, but the offender will abandon the account and take the cash.

Such crimes are often used by petty criminals to obtain funds through a quick embezzlement, and are frequently conducted using a fictitious or stolen identity in order to hide that of the real offender.

This form of fraud is the basis for the Nigerian cheque scam and other similar schemes; however, in these cases, the victim will be the one accused of committing such crimes, and will be left to prove his/her innocence.

Sometimes, forgery is the method of choice in defrauding a bank. One form of forgery involves the use of a victim's legitimate cheques, that have either been altogether stolen and then cashed, or altering a cheque that has been legitimately written to the

perpetrator, by adding words and/or digits in order to inflate the amount (raising a cheque).

Other cases involved the use of completely fake cheques, as in the case of Frank Abagnale. The perpetrator passes or attempts to pass a cheque that has been manufactured by him/herself, but that represents a non-existent account.

Cheque washing involves the theft of a cheque in transit between the writer and recipient, followed by the use of chemicals to remove the ink representing all parts other than the signature. The perpetrator then fills in the blanks to his or her advantage.

Sometimes the cheque fraud comes from an employee of the bank itself, as was the case with Suzette A. Brock, who was convicted of theft for writing five corporate cheques to her own birth name from her desk as a loan servicing agent for Banner Bank of Walla Walla, WA.

The most notorious "bad cheque artist" of the 20th century, Frank Abagnale, devised a scheme to put incorrect MICR numbers at the bottom of the cheque he wrote, so that they would be routed to the incorrect Federal Reserve Bank for clearing. This allowed him to work longer in one area before his criminal activity was detected. In the movie, Catch Me if You Can, which outlines Abagnale's crime spree, it shows Abagnale soaking plastic Pan Am airplanes in his bathtub and removing the Pan Am insignia on the toys. He would then place the decals on the bad cheques he was writing while pretending to be a Pan Am pilot. From his schemes, Abagnale amassed over $2.5 million dollars.

In most jurisdictions, passing a cheque for an amount of money the writer knows is not in the account at the time of negotiation (or available for overdraft protection) is usually considered a violation of criminal law. However, the general practice followed by banks has been to refrain from prosecuting cheque writers if the cheque reaches the bank after sufficient funds have been deposited, thereby allowing it to clear. But the account holder is normally held fully liable for all bank penalties, civil penalties, and criminal charges allowable by law in the event the cheque does not clear the bank.

Only when the successful clearance of a cheque is due to a kiting scheme does the bank traditionally take action. Banks have always had various methods of detecting kiting schemes and stopping them in the act. Computer systems in place will alert bank officials when a customer engages in various suspicious activities, including frequently depositing cheques bearing the same, large monthly total deposits accompanied by near-zero average daily balances, or avoidance of tellers by frequent use of ATMs for deposits.

New technology in place today may make most forms of cheque kiting and paper hanging a thing of the past. As new software rapidly catches illegal activity at the teller/branch level instead of waiting for the nightly runs to the back office, schemes are not only easier to detect, but may be prevented by tellers who deny customers illegal transactions before they are even started.

Part of how banks are combating cheque fraud is to offer their clients fraud protection services. Because it is impossible for banks to know every cheque that a customer writes and which may or may not be fraudulent, the onus is on the clients to make the bank aware of what cheques they write. These systems allow customers to upload their cheque files to the bank including the cheque number, the amount of money, and in some cases, the payee name. Now, when a cheque is presented for payment, the bank scrubs it against the information on file. If one of the variables does not match, then the cheque would be flagged as a potentially fraudulent item.

These services help with external fraud but they do not help if there is internal fraud. If an employee sends information to the bank with fraudulent items, then the bank would not know to deny payment. A system of dual controls should be put into place in order to not allocate all capabilities to one person.

Before the passage of the *Check Clearing for the 21st Century Act*, when cheques could take 3 or more days to clear, *playing the float* was fairly common practice in the USA in otherwise-honest individuals who encountered emergencies right before payday.

Circular and abandonment frauds are gradually being eliminated as cheques will clear in Bank B the same day they are deposited into Bank A, giving no time at all for non-existent funds to become available for withdrawal. With image-sharing technology, the funds that temporarily become available in Bank A's account are wiped out the same day.

While there may still be some room for retail kiting, security measures taken by retail chains are helping reduce such incidents. Increasingly, more chains are limiting the amount of cash back received, the number of times cash back can be offered in a week or a given period of time, and obtaining transactional account balances before offering cash back, thereby denying it to those with low balances. For example, Walmart's policy is to determine account balances of those obtaining cash back, and some Safeway locations will not offer cash back on any accounts with balances under $250, even when funds are sufficient to cover the amount on the cheque. Customers who are noted to obtain cash back frequently are also investigated by the corporation to observe patterns.

Some businesses will also use the cheque strictly as an informational device to automatically debit funds from the account, and will return the item to the customer thereafter. However, in the United Statesthis is done through the Automated Clearing House (ACH); though faster than traditional check clearing, contrary to popular belief the ACH is not instantaneous. Though this practice reduces the room for kiting (by reducing float), it does not always eliminate it.

Insurance fraud

Insurance fraud is any act committed with the intent to obtain a fraudulent outcome from an insurance process. This may occur when a claimant attempts to obtain some benefit or advantage to which they are not otherwise entitled, or when an insurer knowingly denies some benefit that is due. According to the United States Federal Bureau of Investigation the most common schemes include: Premium Diversion, Fee Churning, Asset Diversion, and Workers Compensation Fraud. The perpetrators in these schemes can be both insurance company employees and claimants. **False insurance claims** are insuranceclaims filed with the intent to defraud an insurance provider.

Insurance fraud has existed since the beginning of insurance as a commercial enterprise. Fraudulent claims account for a significant portion of all claims received by insurers, and cost billions of dollars annually. Types of insurance fraud are diverse, and occur in all areas of insurance. Insurance crimes also range in severity, from slightly exaggerating claims to deliberately causing accidents or damage. Fraudulent activities affect the lives of innocent people, both directly through accidental or intentional injury or damage, and indirectly as these crimes cause insurance premiums to be higher. Insurance fraud poses a significant problem, and governments and other organizations make efforts to deter such activities.

An epigram by the Roman poet Martial provides a clear evidence the phenomenon of insurance fraud was already known in the Roman Empire during the First Century AD :

> "Tongilianus, you paid two hundred for your house;
> An accident too common in this city destroyed it.
> You collected ten times more. Doesn't it seem, I pray,
> That you set fire to your own house, Tongilianus?"
> *Book III, No. 52*

The “chief motive in all insurance crimes is financial profit.” Insurance contracts provide both the insured and the insurer with opportunities for exploitation.

According to the Coalition Against Insurance Fraud, the causes vary, but are usually centered on greed, and on holes in the protections against fraud. Often, those who commit insurance fraud view it as a low-risk, lucrative enterprise. For example, drug dealers who have entered insurance fraud think it’s safer and more profitable than

working street corners. Compared to those for other crimes, court sentences for insurance fraud can be lenient, reducing the risk of extended punishment. Though insurers try to fight fraud, some will pay suspicious claims anyway; settling such claims is often cheaper than legal action.

Another reason for fraud is over-insurance, when the amount insured is greater than the actual value of the property insured. This condition can be very difficult to avoid, especially since an insurance provider might sometimes encourage it in order to obtain greater profits. This allows fraudsters to make profits by destroying their property because the payment they receive from their insurers is of greater value than the property they destroy. The most common forms of insurance fraud are reframing a non-insured damage in order to make it an event covered by insurance and inflating the value of the loss.

Insurance companies are also susceptible to fraud because it's possible for fraudsters to file claims for damages that never occurred.

It is hard to place an exact value on the money stolen through insurance fraud. Insurance fraud is deliberately undetectable, unlike visible crimes such as robbery or murder. As such, the number of cases of insurance fraud that are detected is much lower than the number of acts that are actually committed. The best that can be done is to provide an estimate for the losses that insurers suffer due to insurance fraud. The Coalition Against Insurance Fraud estimates that in 2006 a total of about $80 billion was lost in the United States due to insurance fraud. According to estimates by the Insurance Information Institute, insurance fraud accounts for about 10 percent of the property/casualty insurance industry’s incurred losses and loss adjustment expenses. The National Health Care Anti-Fraud Association estimates that 3% of the health care industry’s expenditures in the United States are due to fraudulent activities, amounting to a cost of about $51 billion. Other estimates attribute as much as 10% of the total healthcare spending in the United States to fraud—about $115 billion annually. Another study of all types of fraud committed in the United States insurance institutions (property-and-casualty, business liability, healthcare, social security, etc.)put the true cost at 33% to 38% of the total cash flow through the system. This study resulted in the book title "The Trillion Dollar Insurance Crook" by J.E. Smith. In the United Kingdom, the Insurance Fraud Bureau estimates that the loss due to insurance fraud in the United Kingdom is about £1.5 billion ($3.08 billion), causing a 5% increase in insurance premiums. The Insurance Bureau of Canada estimates that personal injury fraud in Canada costs about C$500 million annually. Indiaforensic Center of Studies estimates that Insurance frauds in India costs about $6.25 billion annually.

Insurance fraud can be classified as either hard fraud or soft fraud.

Hard fraud occurs when someone deliberately plans or invents a loss, such as a collision, auto theft, or fire that is covered by their insurance policy in order to receive payment for damages. Criminal rings are sometimes involved in hard fraud schemes that can steal millions of dollars.

Soft fraud, which is far more common than hard fraud, is sometimes also referred to as opportunistic fraud. This type of fraud consists of policyholders exaggerating otherwise-legitimate claims. For example, when involved in an automotive collision an insured person might claim more damage than actually occurred. Soft fraud can also occur when, while obtaining a new health insurance policy, an individual misreports previous or existing conditions in order to obtain a lower premium on his or her insurance policy.

Life insurance fraud may involve faking death to claim life insurance. Fraudsters may sometimes turn up a few years after disappearing, claiming a loss of memory.

An example of life insurance fraud is the John Darwin disappearance case, which was an investigation into the act of pseudocide committed by the British former teacher and prison officer John Darwin, who turned up alive in December 2007, five years after he was thought to have died in a canoeing accident. Darwin was reported as "missing" after failing to report to work following a canoeing trip on March 21, 2002. He reappeared on December 1, 2007, claiming to have no memory of the past five years.

Another example is former British Government minister John Stonehouse who went missing in 1974 from a beach in Miami. He was discovered living under an assumed name in Australia, extradited to Britain and jailed for seven years for fraud, theft and forgery.

Health insurance fraud is described as an intentional act of deceiving, concealing, or misrepresenting information that results in health care benefits being paid to an individual or group.

Fraud can be committed either by an insured person or by a provider. Member fraud consists of claims on behalf of ineligible members and/or dependents, alterations on enrollment forms, concealing pre-existing conditions, failure to report other coverage, prescription drug fraud, and failure to disclose claims that were a result of a work-related injury.

Provider fraud consists of claims submitted by bogus physicians, billing for services not rendered, billing for higher level of services, diagnosis or treatments that are outside the scope of practice, alterations on claims submissions, and providing services while medical licenses are either suspended or revoked. Independent medical examinations debunk false insurance claims and allow the insurance company or claimant to seek a non-partial medical view for injury-related cases.

According to the Coalition Against Insurance Fraud, health insurance fraud depletes taxpayer-funded programs like Medicare, and may victimize patients in the hands of certain doctors. Some scams involve double-billing by doctors who charge insurers for treatments that never occurred, and surgeons who perform unnecessary surgery.

According to Roger Feldman, Blue Cross Professor of Health Insurance at the University of Minnesota, one of the main reasons that medical fraud is such a prevalent practice is that nearly all of the parties involved find it favorable in some way. Many physicians see it as necessary to provide quality care for their patients. Many patients, although disapproving of the idea of fraud, are sometimes more willing to accept it when it affects their own medical care. Program administrators are often lenient on the issue of insurance fraud, as they want to maximize the services of their providers.

The most common perpetrators of healthcare insurance fraud are health care providers. One reason for this, according to David Hyman, a Professor at the University of Maryland School of Law, is that the historically-prevailing attitude in the medical profession is one of “fidelity to patients”. This incentive can lead to fraudulent practices such as billing insurers for treatments that are not covered by the patient’s insurance policy. To do this, physicians often bill for a different service, which is covered by the policy, rather than that which they rendered.

Another motivation for insurance fraud is a desire for financial gain. Public healthcare programs such as Medicare and Medicaid are especially conducive to fraudulent activities, as they are often run on a fee-for-service structure. Physicians use several fraudulent techniques to achieve this end. These can include “up-coding” or “upgrading,” which involve billing for more expensive treatments than those actually provided; providing, and subsequently billing for, treatments that are not medically necessary; scheduling extra visits for patients; referring patients to other physicians when no further treatment is actually necessary; "phantom billing," or billing for services not rendered; and “ganging,” or billing for services to family members or other individuals who are accompanying the patient but who did not personally receive any services.

Perhaps the greatest total dollar amount of fraud is committed by the health insurance companies themselves. There are numerous studies and articles detailing examples of insurance companies intentionally not paying claims and deleting them from their systems, denying and cancelling coverage, and the blatant underpayment to hospitals and physicians beneath what are normal fees for care they provide. Although difficult to obtain the information, this fraud by insurance companies can be estimated by comparing revenues from premium payments and expenditures on health claims.

In response to the increased amount of health care fraud in the United States, Congress, through the Health Insurance Portability and Accountability Act of 1996 (HIPAA), has specifically established health care fraud as a federal criminal offense with punishment of up to ten years of prison in addition to significant financial penalties.

Automobile insurance

Fraud rings or groups may fake traffic deaths or stage collisions to make false insurance or exaggerated claims and collect insurance money. The ring may involve insurance claims adjusters and other people who create phony police reports to process claims.

The Insurance Fraud Bureau in the UK estimated there have already been more than 20,000 staged collisions and false insurance claims across the UK from 1999 to 2006. One tactic fraudsters use is to drive to a busy junction or roundabout and brake sharply causing a motorist to drive into the back of them. They claim the other motorist was at fault because they were driving too fast or too close behind them, and make a false and inflated claim to the motorist's insurer for whiplash and damage which can give the fraudsters up to £30,000. In the Insurance Fraud Bureau's first year or operation, the usage of data mining initiatives exposed insurance fraud networks and led to 74 arrests and a five-to-one return on investment.

The Insurance Research Council estimated that in 1996, 21 to 36 percent of auto-insurance claims contained elements of suspected fraud. There is a wide variety of schemes used to defraud automobile insurance providers. These ploys can differ greatly in complexity and severity. Richard A. Derrig, vice president of research for the Insurance Fraud Bureau of Massachusetts, lists several ways that auto-insurance fraud can occur, such as:

Staged collisions

In staged collision fraud, fraudsters use a motor vehicle to stage an accident with the innocent party. Typically, the fraudsters' vehicle carries four or five passengers. Its

driver makes an unexpected manoeuvre, forcing an innocent party to collide with the fraudster's vehicle. Each of the fraudsters then files claims for injuries sustained in the vehicle. A “recruited” doctor diagnoses whiplash or other soft-tissue injuries which are hard to dispute later.

Other examples include jumping in front of cars as done in Russia. The driving conditions and roads are dangerous with many people trying to scam drivers by jumping in front of expensive-looking cars or crashing into them. Hit and runs are very common and insurance companies notoriously specialize in denying claims. Two-way insurance coverage is very expensive and almost completely unavailable for vehicles over ten years old–the drivers can only obtain basic liability. Because Russian courts do not like using verbal claims, most people have dashboard cameras installed to warn would-be perpetrators or provide evidence for/against claims.

Exaggerated claims

A real accident may occur, but the dishonest owner may take the opportunity to incorporate a whole range of previous minor damage to the vehicle into the garage bill associated with the real accident. Personal injuries may also be exaggerated, particularly whiplash. Insurance fraud cases of exaggerated claims can also include claiming damage to the car that did not result from the accident for which the claim is made.

Examples

Examples of soft auto-insurance fraud can include filing more than one claim for a single injury, filing claims for injuries not related to an automobile accident, misreporting wage losses due to injuries, or reporting higher costs for car repairs than those that were actually paid. Hard auto-insurance fraud can include activities such as staging automobile collisions, filing claims when the claimant was not actually involved in the accident, submitting claims for medical treatments that were not received, or inventing injuries. Hard fraud can also occur when claimants falsely report their vehicle as stolen. Soft fraudaccounts for the majority of fraudulent auto-insurance claims.

Another example is that a person may illegally register their car to a location that would net them cheaper insurance rates than where they actually live, sometimes called "rate evasion". For example, some drivers in Brooklyn drive with Pennsylvania license plates because registering their car in a rural part of Pennsylvania will cost a lot less than registering it in Brooklyn. Another form of automobile insurance fraud, known as "fronting," involves registering someone other than the real primary driver

of a car as the primary driver of the car. For example, parents might list themselves as the primary driver of their children's vehicles to avoid young driver premiums.

"Crash for cash" scams may involve random unaware strangers, set to appear as the perpetrators of the orchestrated crashes. Such techniques are the *classic rear-end shunt* (the driver in front suddenly slams on the brakes, possibly with brake lights disabled), the *decoy rear-end shunt* (when following one car, another one pulls in front of it, causing it to brake sharply, then the first car drives off) or the *helpful wave shunt* (the driver is waved into a line of queuing traffic by the scammer who promptly crashes, then denies waving).

Organized crime rings can also be involved in auto-insurance fraud, sometimes carrying out schemes that are very complex. An example of one such ploy is given by Ken Dornstein, author of *Accidentally, on Purpose: The Making of a Personal Injury Underworld in America*. In this scheme, known as a “swoop-and-squat,” one or more drivers in “swoop” cars force an unsuspecting driver into position behind a “squat” car. This squat car, which is usually filled with several passengers, then slows abruptly, forcing the driver of the chosen car to collide with the squat car. The passengers in the squat car then file a claim with the other driver’s insurance company. This claim often includes bills for medical treatments that were not necessary or not received.

An incident that took place on Golden State Freeway June 17, 1992, brought public attention to the existence of organized crime rings that stage auto accidents for insurance fraud. These schemes generally consist of three different levels. At the top, there are the professionals—doctors or lawyers who diagnose false injuries and/or file fraudulent claims and these earn the bulk of the profits from the fraud. Next are the "capper (insurance fraud)s" or "runners", the middlemen who obtain the cars to crash, farm out the claims to the professionals at the top, and recruit participants. These participants at the bottom-rung of the scheme are desperate people (poor immigrants or others in need of quick cash) who are paid around $1000 USD to place their bodies in the paths of cars and trucks, playing a kind of Russian roulette with their lives and those of unsuspecting motorists around them. According to investigators, cappers usually hire within their own ethnic groups. What makes busting these staged-accident crime ringsdifficult is how quickly they move into jurisdictions with lesser enforcement, after a crackdown in a particular region. As a result, in the US several levels of police and the insurance industry have cooperated in forming task forces and sharing databases to track claim histories.

In the United Kingdom, there is an increasing incidence of false whiplash claims to car insurance companies from motorists involved in minor car accidents (for instance; a shunt). Because the mechanism of injury is not fully

understood, A&E doctors have to rely on a patient's external symptoms (which are easy to fake). Resultingly, "no win no fee" personal injury solicitors exploit this "loophole" for easy compensation money (often a £2500 payout). Ultimately this has resulted in increased motor insurance premiums, which has had the knock-on effect of pricing younger drivers off the road.

Property insurance

Possible motivations for this can include obtaining payment that is worth more than the value of the property destroyed, or to destroy and subsequently receive payment for goods that could not otherwise be sold. According to Alfred Manes, the majority of property insurance crimes involve arson. One reason for this is that any evidence that a fire was started by arson is often destroyed by the fire itself. According to the United States Fire Administration, in the United States there were approximately 31,000 fires caused by arson in 2006, resulting in losses of $755 million.

Council compensation claims

The fraud involving claims from the councils' insurers suppose staging damages blamable on the local authorities (mostly falls and trips on council owned land) or inflating the value of existing damages.

Detecting insurance fraud

The detection of insurance fraud generally occurs in two steps. The first step is to identify suspicious claims that have a higher possibility of being fraudulent. This can be done by computerized statisticalanalysis or by referrals from claims adjusters or insurance agents. Additionally, the public can provide tips to insurance companies, law enforcement and other organizations regarding suspected, observed, or admitted insurance fraud perpetrated by other individuals. Regardless of the source, the next step is to refer these claims to investigators for further analysis.

Due to the sheer number of claims submitted each day, it would be far too expensive for insurance companies to have employees check each claim for symptoms of fraud. Instead, many companies use computers and statistical analysis to identify suspicious claims for further investigation. There are two main types of statistical analysis tools used: supervised and unsupervised. In both cases, suspicious claims are identified by comparing data about the claim to expected values. The main difference between the two methods is how the expected values are derived.

In a supervised method, expected values are obtained by analyzing records of both fraudulent and non-fraudulent claims. According to Richard J. Bolton and David B.

Hand, both of Imperial College in London, this method has some drawbacks as it requires absolute certainty that those claims analyzed are actually either fraudulent or non-fraudulent, and because it can only be used to detect types of fraud that have been committed and identified before.

Unsupervised methods of statistical detection, on the other hand, involve detecting claims that are abnormal. Both claims adjusters and computers can also be trained to identify “red flags,” or symptoms that in the past have often been associated with fraudulent claims. Statistical detection does not prove that claims are fraudulent; it merely identifies suspicious claims that need to be investigated further.

Fraudulent claims can be one of two types. They can be otherwise legitimate claims that are exaggerated or “built up,” or they can be false claims in which the damages claimed never actually occurred. Once a built up claim is identified, insurance companies usually try to negotiate the claim down to the appropriate amount. Suspicious claims can also be submitted to “special investigative units”, or SIUs, for further investigation. These units generally consist of experienced claims adjusters with special training in investigating fraudulent claims. These investigators look for certain symptoms associated with fraudulent claims, or otherwise look for evidence of falsification of some kind. This evidence can then be used to deny payment of the claims or to prosecute fraudsters if the violation is serious enough.

Once an insurance company's fraud investigation department is assigned to investigate a fraud claim, they will frequently proceed with the investigation in two stages: pre-contact and post-contact. The first, pre-contact stage involves analyzing all available evidence before the suspect is contacted. This may involve reviewing paperwork submitted, reaching out to third parities, and gathering evidence from available sources. The second stage, "post-contact," involves initiating contact with the suspect to gather more information and, ideally, obtain an incriminating statement. Insurance fraud investigators are trained to question the suspect in a manner that would preclude the possibility of the suspect raising a valid defense at a later time. For example, questions about access to claim forms would preclude the defense that another individual filled out the fraudulent documents. Common defenses that may be precluded by the suspect interview include, for example, that the suspect lacked knowledge that his or her statement was false, lacked the intention to defraud another individual, or made an ambiguous statement that was later interpreted incorrectly. Full disclosure may add credibility to a suspect's account of events, but omissions from disclosure or false statements may detract from the suspect's credibility in later interviews or proceedings.

In the health insurance fraud context, determining fraud committed by the health insurance companies can also sometimes be found by comparing revenues from premiums paid against the expenditure by the health insurance companies on claims.

As an example, in 2006 the Harris County Medical Society, in Texas, had a health insurance rate increase of 22 percent for "consumer-driven" health plan from Blue Cross and Blue Shield of Texas. This was despite the fact that during the previous year Blue Cross had paid out only 9 percent of the collected premium dollars for claims.

Legislation

National and local governments, especially in the last half of the twentieth century, have recognized insurance fraud as a serious crime, and have made efforts to punish and prevent this practice. Some major developments are listed below:

United States

- Insurance Fraud is specifically classified as a crime in all states, though a minority of states only criminalize certain types (e.g. Oregon only outlaws Worker Compensation and Property Claim fraud).
- The Coalition Against Insurance Fraud was founded in 1993 to help fight insurance fraud. This organization collects information on insurance fraud, and is the only anti-fraud alliance speaking for consumers, insurance companies, government agencies and others. Through its unique work, the Coalition empowers consumers to fight back, helps fraud fighters better detect this crime and deters more people from committing fraud. The Coalition supports this mission with a large and continually expanding armory of practical tools: Information, research & data, services and insight as a leading voice of the anti-fraud community.
- Approximately one third of these investigations result in criminal conviction, one third result in denial of the claim, and one third result in payment of the claim.
- 19 states require mandatory insurer fraud plans. This requires companies to form programs to combat fraud and in some cases to develop investigation units to detect fraud.
- 41 states have fraud bureaus. These are law enforcement agencies where "investigators review fraud reports and begin the prosecution process."
- Section 1347 of Title 18 of the United States Code states that whoever attempts or carries out a "scheme or artifice" to "defraud a health care benefit program"

will be “fined under this title or imprisoned not more than 10 years, or both.” If this scheme results in bodily injury, the violator may be imprisoned up to 20 years, and if the scheme results in death the violator may be imprisoned for life.

Besides making laws more severe, Legislation has also come up with a list for management that should be implemented so that companies are better suited to combat the possibility of being scammed. That list includes:

- Understanding that fraud does exist and that there is a high possibility for it happening.
- Being fully aware of the dangers and severity of the problem.
- Understanding the importance of the hiring process and how important it is to hire honest individuals.
- Learn to deal with the economic side of business. That means putting procedures and policies in place to catch and deal with individuals trying to commit fraud.

Canada

- The Insurance Crime Prevention Bureau was founded in 1973 to help fight insurance fraud. This organization collects information on insurance fraud, and also carries out investigations. Approximately one third of these investigations result in criminal conviction, one third result in denial of the claim, and one third result in payment of the claim.
- British Columbia’s Traffic Safety Statutes Amendment Act of 1997 states that any person who submits a motor vehicle insurance claim that contains false or misleading information may on the first offence be fined C$25,000, imprisoned for two years, or both. On the second offense, that person may be fined C$50,000, imprisoned for two years, or both.

United Kingdom

- A major portion of the Financial Services Act 1986 was intended to help prevent fraud.
- The Serious Fraud Office, set up under the Criminal Justice Act 1987, was established to “improve the investigation and prosecution of serious and complex fraud.”
- The Fraud Act 2006 specifically defines fraud as a crime. This act defines fraud as being committed when a person “makes a false representation,” “fails to disclose to another person information which he is under a legal duty to disclose,” or abuses a position in which he or she is “expected to safeguard, or

not to act against, the financial interests of another person." This act also defines the penalties for fraud as imprisonment up to ten years, a fine, or both.

Securities fraud

Securities fraud, also known as **stock fraud** and **investment fraud**, is a deceptive practice in the stock or commodities markets that induces investors to make purchase or sale decisions on the basis of false information, frequently resulting in losses, in violation of securities laws. Offers of risky investment opportunities to unsophisticated investors who are unable to evaluate risk adequately and cannot afford loss of capital is a central problem.

Securities fraud can also include outright theft from investors (embezzlement by stockbrokers), stock manipulation, misstatements on a public company's financial reports, and lying to corporate auditors. The term encompasses a wide range of other actions, including insider trading, front running and other illegal acts on the trading floor of a stock or commodity exchange.

Fraud by high level corporate officials became a subject of wide national attention during the early 2000s, as exemplified by corporate officer misconduct at Enron. It became a problem of such scope that the Bush Administration announced what it described as an "aggressive agenda" against corporate fraud. Less widely publicized manifestations continue, such as the securities fraud conviction of Charles E. Johnson Jr., founder of PurchasePro in May 2008. FBI Director Robert Mueller predicted in April 2008 that corporate fraud cases will increase because of the subprime mortgage crisis.

Dummy corporations may be created by fraudsters to create the illusion of being an existing corporation with a similar name. Fraudsters then sell securities in the dummy corporation by misleading the investor into thinking that they are buying shares in the real corporation.

According to enforcement officials of the Securities and Exchange Commission, criminals engage in pump-and-dump schemes, in which false and/or fraudulent information is disseminated in chat rooms, forums, internet boards and via email (spamming), with the purpose of causing a dramatic price increase in thinly traded stocks or stocks of shell companies (the "pump").

When the price reaches a certain level, criminals immediately sell off their holdings of those stocks (the "dump"), realizing substantial profits before the stock price falls back to its usual low level. Any buyers of the stock who are unaware of the fraud become victims once the price falls.

The SEC says that Internet fraud resides in several forms:

- Online investment newsletters that offer seemingly unbiased information free of charge about featured companies or recommending "stock picks of the month." These newsletter writers then sell shares, previously acquired at lower prices, when hype-generated buying drives the stock price up. This practice is known as scalping. Conflict of interest disclosures incorporated into a newsletter article may not be sufficient. Accused of scalping, Thom Calandra, formerly of MarketWatch, was the subject of an SEC enforcement action in 2004.
- Bulletin boards that often contain fraudulent messages by hucksters.
- E-Mail spams from perpetrators of fraud.
- Phishing

Insider trading

There are two types of "insider trading". The first is the trading of a corporation's stock or other security by corporate insiders such as officers, key employees, directors, or holders of more than ten percent of the firm's shares. This is generally legal, but there are certain reporting requirements.

The other type of insider trading is the purchase or sale of a security based on material non-public information. This type of trading is illegal in most instances. In illegal insider trading, an insider or a related party trades based on material non-public information obtained during the performance of the insider's duties at the corporation, or otherwise misappropriated.

Microcap fraud

In microcap fraud, stocks of small companies of under $250 million market capitalization are deceptively promoted, then sold to an unwary public. This type of fraud has been estimated to cost investors $1–3 billion annually. Microcap fraud includes pump and dump schemes involving boiler rooms and scams on the Internet. Many, but not all, microcap stocks involved in frauds are penny stocks, which trade for less than $5 a share.

Many penny stocks, particularly those that sell for fractions of a cent, are thinly traded. They can become the target of stock promoters and manipulators. These manipulators first purchase large quantities of stock, then artificially inflate the share price through false and misleading positive statements. This is referred to as a pump

and dump scheme. The pump and dump is a form of microcap stock fraud. In more sophisticated versions of the fraud, individuals or organizations buy millions of shares, then use newsletter websites, chat rooms, stock message boards, press releases, or e-mail blasts to drive up interest in the stock. Very often, the perpetrator will claim to have "inside" information about impending news to persuade the unwitting investor to quickly buy the shares. When buying pressure pushes the share price up, the rise in price entices more people to believe the hype and to buy shares as well. Eventually the manipulators doing the "pumping" end up "dumping" when they sell their holdings. The expanding use of the Internet and personal communication devices has made penny stock scams easier to perpetrate. But it has also drawn high-profile public personalities into the sphere of regulatory oversight. Though not a scam per se, one notable example is rapper 50 Cent's use of Twitter to cause the price of a penny stock (HNHI) to increase dramatically. 50 Cent had previously invested in 30 million shares of the company, and as a result made $8.7 million in profit. Another example of an activity that skirts the borderline between legitimate promotion and hype is the case of LEXG. Described (but perhaps overstated) as "the biggest stock promotion of all time", Lithium Exploration Group's market capitalization soared to over $350 million, after an extensive direct mail campaign. The promotion drew upon the legitimate growth in production and use of lithium, while touting Lithium Exploration Groups position within that sector. According to the company's December 31, 2010, form 10-Q (filed within months of the direct mail promotion), LEXG was a lithium company without assets. Its revenues and assets at that time were zero. Subsequently, the company did acquire lithium production/exploration properties, and addressed concerns raised in the press.

Penny stock companies often have low liquidity. Investors may encounter difficulty selling their positions after the buying pressure has abated, and the manipulators have fled.

Accountant fraud

In 2002, a wave of separate but often related accounting scandals became known to the public in the U.S. All of the leading public accounting firms—Arthur Andersen, Deloitte & Touche, Ernst & Young, KPMG, PricewaterhouseCoopers— and others have admitted to or have been charged with negligence to identify and prevent the publication of falsified financial reports by their corporate clients which had the effect of giving a misleading impression of their client companies' financial status. In several cases, the monetary amounts of the fraud involved are in the billions of USD.

Boiler rooms

Boiler rooms or boiler houses are stock brokerages that put undue pressure on clients to trade using telesales, usually in pursuit of microcap fraud schemes. Some boiler rooms offer clients transactions fraudulently, such as those with an undisclosed profitable relationship to the brokerage. Some 'boiler rooms' are not licensed but may be 'tied agents' of a brokerage house which itself is licensed or not. Securities sold in boiler rooms include commodities and private placements as well as microcap stocks, non-existent, or distressed stock and stock supplied by an intermediary at an undisclosed markup.

Mutual Fund fraud

A number of major brokerages and mutual fund firms were accused of various deceptive acts that disadvantaged customers. Among them were late trading and market timing. Various SEC rules were enacted to curtail this practice. Bank of America Capital Management was accused by the SEC of having undisclosed arrangements with customers to allow short term trading.

Short selling abuses

Abusive short selling, including certain types of naked short selling, are also considered securities fraud because they can drive down stock prices. In abusive naked short selling, stock is sold without being borrowed and without any intent to borrow. The practice of spreading false information about stocks, to drive down their prices, is called "short and distort." During the takeover of Bear Stearns by J.P. Morgan Chase in March 2008, reports swirled that shorts were spreading rumors to drive down Bear Stearns' share price. Sen. Christopher Dodd, D-Conn., said this was more than rumors and said, "This is about collusion."

Ponzi schemes

A Ponzi scheme is an investment fund where withdrawals are financed by subsequent investors, rather than profit obtained through investment activities. The largest instance of securities fraud committed by an individual ever is a Ponzi scheme operated by former NASDAQ chairman Bernard Madoff, which caused up to an estimated $64.8 billion in losses depending on which method is used to calculate the losses prior to its collapse.

Pervasiveness of securities fraud

The Securities Investor Protection Corporation (SIPC) reports that the Federal Trade Commission, FBI, and state securities regulators estimate that investment fraud in the United States ranges from $10–$40 billion annually. Of that number, SIPC estimates that $1–3 Billion is directly attributable to microcap stock fraud. Fraudulent schemes perpetrated in the securities and commodities markets can ultimately have a devastating impact on the viability and operation of these markets.

Class action securities fraud lawsuits rose 43 percent between 2006 and 2007, according to the Stanford Law School Securities Class Action Clearinghouse. During 2006 and 2007, securities fraud class actions were driven by market wide events, such as the 2006 backdating scandal and the 2007 subprime crisis. Securities fraud lawsuits remained below historical averages.

Some manifestations of this white collar crime have become more frequent as the Internet gives criminals greater access to prey. The trading volume in the United States securities and commodities markets, having grown dramatically in the 1990s, has led to an increase in fraud and misconduct by investors, executives, shareholders, and other market participants.

Securities fraud is becoming more complex as the industry develops more complicated investment vehicles. In addition, white collar criminals are expanding the scope of their fraud and are looking outside the United States for new markets, new investors, and banking secrecy havens to hide unjust enrichment.

A study conducted by the New York Stock Exchange in the mid-1990s reveals approximately 51.4 million individuals owned some type of traded stock, while 200 million individuals owned securities indirectly. These same financial markets provide the opportunity for wealth to be obtained and the opportunity for white collar criminals to take advantage of unwary investors.

Recovery of assets from the proceeds of securities fraud is a resource intensive and expensive undertaking because of the cleverness of fraudsters in concealment of assets and money laundering, as well as the tendency of many criminals to be profligate spenders. A victim of securities fraud is usually fortunate to recover any money from the defrauder.

Sometimes the losses caused by securities fraud are difficult to quantify. For example, insider trading is believed to raise the cost of capital for securities issuers, thus decreasing overall economic growth.

Characteristics of victims and perpetrators

Any investor can become a victim, but persons aged fifty years or older are most often victimized, whether as direct purchasers in securities or indirect purchasers through pension funds. Not only do investors lose but so can creditors, taxing authorities, and employees.

Potential perpetrators of securities fraud within a publicly traded firm include any dishonest official within the company who has access to the payroll or financial reports that can be manipulated to:

1. overstate assets
2. overstate revenues
3. understate costs
4. understate liabilities
5. understate pennystock

Enron Corporation exemplifies all five tendencies, and its failure demonstrates the extreme dangers of a culture of corruption within a publicly traded corporation. The rarity of such spectacular failures of a corporation from securities fraud attests to the general reliability of most executives and boards of large corporations. Most spectacular failures of publicly traded companies result from such innocent causes as marketing blunders (Schlitz), an obsolete model of business (Penn Central, Woolworth's), inadequate market share (Studebaker), non-criminal incompetence (Braniff).

Other effects of securities fraud

Even if the effect of securities fraud is not enough to cause bankruptcy, a lesser level can wipe out holders of common stock because of the leverage of value of shares upon the difference between assets and liabilities. Such fraud has been known as watered stock, analogous to the practice of force-feeding livestock great amounts of water to inflate their weight before sale to dealers.

Penny stock regulation

The regulation and prosecution of securities fraud violations is undertaken on a broad front, involving numerous government agencies and self-regulatory organizations. One method of regulating and restricting a specific type of fraud perpetrated by pump and dump manipulators, is to target the category of stocks most often associated with this scheme. To that end, penny stocks have been the target of heightened enforcement efforts. In the United States, regulators have defined a penny stock as a

security that must meet a number of specific standards. The criteria include price, market capitalization, and minimum shareholder equity. Securities traded on a national stock exchange, regardless of price, are exempt from regulatory designation as a penny stock, since it is thought that exchange traded securities are less vulnerable to manipulation. Therefore, CitiGroup (NYSE:C) and other NYSE listed securities which traded below $1.00 during the market downturn of 2008–2009, while properly regarded as "low priced" securities, were not technically "penny stocks". Although penny stock trading in the United States is now primarily controlled through rules and regulations enforced by the United States Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA), the genesis of this control is found in State securities law. The State of Georgia was the first state to codify a comprehensive penny stock securities law. Secretary of State Max Cleland, whose office enforced State securities laws was a principal proponent of the legislation. Representative Chesley V. Morton, the only stockbroker in the Georgia General Assembly at the time, was principal sponsor of the bill in the House of Representatives. Georgia's penny stock law was subsequently challenged in court. However, the law was eventually upheld in U.S. District Court, and the statute became the template for laws enacted in other states. Shortly thereafter, both FINRA and the SEC enacted comprehensive revisions of their penny stock regulations. These regulations proved effective in either closing or greatly restricting broker/dealers, such as Blinder, Robinson & Company, which specialized in the penny stocks sector. Meyer Blinder was jailed for securities fraud in 1992, after the collapse of his firm. However, sanctions under these specific regulations lack an effective means to address pump and dumpschemes perpetrated by unregistered groups and individuals.

Counterfeit

To **counterfeit** means to imitate something. Counterfeit products are fakes or unauthorized replicas of the real product. Counterfeit products are often produced with the intent to take advantage of the superior value of the imitated product. The word *counterfeit* frequently describes both the forgeries of currency and documents, as well as the imitations of items such as clothing, handbags, shoes, pharmaceuticals, aviation and automobile parts, watches, electronics (both parts and finished products), software, works of art, toys, and movies.

Counterfeit products tend to have fake company logos and brands (resulting in patent or trademark infringement in the case of goods), have a reputation for being lower quality (sometimes not working at all) and may even include toxic elements such as lead. This has resulted in the deaths of hundreds of thousands of people, due to automobile and aviation accidents, poisoning, or ceasing to take essential compounds (e.g., in the case a person takes non-working medicine).

The counterfeiting of money is usually attacked aggressively by governments worldwide. Paper money is the most popular product counterfeited.

Counterfeit money is currency that is produced without the legal sanction of the state or government and in deliberate violation of that country's laws.

The United States Secret Service, mostly known for its guarding-of-officials task, was initially organized primarily to combat the counterfeiting of American money. Counterfeit government bonds are public debt instruments that are produced without legal sanction, with the intention of "cashing them in" for authentic currency or using them as collateral to secure legitimate loans or lines of credit.

Forgery is the process of making or adapting documents with the intention to deceive. It is a form of fraud, and is often a key technique in the execution of identity theft. Uttering and publishing is a term in United States law for the forgery of non-official documents, such as a trucking company's time and weight logs.

Questioned document examination is a scientific process for investigating many aspects of various documents, and is often used to examine the provenance and verity of a suspected forgery. Security printingis a printing industry specialty, focused on creating legal documents which are difficult to forge.

The spread of counterfeit goods (commonly called "knock-offs" or "rip-offs") has become global in recent years and the range of goods subject to infringement has

increased significantly. Apparel and accessories accounted for over 50 percent of the counterfeit goods seized by U.S Customs and Border Control. According to the study of Counterfeiting Intelligence Bureau (CIB) of the International Chamber of Commerce (ICC), counterfeit goods make up 5 to 7% of World Trade; however, these figures cannot be substantiated due to the secretive nature of the industry.

A report by the Organisation for Economic Co-operation and Development indicates that up to US$200 Billion of international trade could have been in counterfeit and illegally copied goods in 2005. In November 2009, the OECD updated these estimates, concluding that the share of counterfeit and illegitimate goods in world trade had increased from 1.85% in 2000 to 1.95% in 2007. That represents an increase to US$250 billion worldwide.

In a detailed breakdown of the counterfeit goods industry, the total loss faced by countries around the world is $600 billion, with the United States facing the most economic impact. When calculating counterfeit products, current estimates place the global losses at $400 billion. On November 29, 2010, the Department of Homeland Security seized and shut down 82 websites as part of a U.S. crackdown of websites that sell counterfeit goods, and was timed to coincide with "Cyber Monday," the start of the holiday online shopping season.

Some see the rise in counterfeiting of goods as being related to globalisation. As more and more companies, in an effort to increase profits, move manufacturing to the cheaper labour markets of the third world, areas with weaker labour laws or environmental regulations, they give the means of production to foreign workers. These new managers of production have little or no loyalty to the original corporation. They see that profits are being made by the global brand for doing little (other than advertising) and see the possibilities of removing the middle men (i.e. the parent corporation) and marketing directly to the consumer. This can result in counterfeit products being virtually indistinguishable from original products, as they are being produced in the same company, and in damage to the parent corporation due to copyright infringement.

Certain consumer goods, especially very expensive or desirable brands or those that are easy to reproduce cheaply, have become frequent and common targets of counterfeiting. The counterfeiters either attempt to deceive the consumer into thinking they are purchasing a legitimate item, or convince the consumer that they could deceive others with the imitation. An item which makes no attempt to deceive, such as a copy of a DVD with missing or different cover art or a book without a cover, is often called a "bootleg" or a "pirated copy" instead.

Counterfeiting has also been issued to "cash in" on the ever growing record collecting market. One major example is bootleggers have cloned copies of Elvis Presley's early singles for Sun Records since original copies starting changing hands amongst music fans for hundreds (and then, thousands) of US$. Some who produce these even do so with the wrong material. For example the song "Heartbreak Hotel" which was never released on Sun, as by the time Elvis' first heard it, prior to ever recording it, he had moved from Sun to RCA Victor. Rare releases by The Beatles such as their album with the butcher cover, fan-club only released Christmas records and early demonstration discs issued by EMI are also examples of product reproduced by counterfeiters due to their high value to collectors.

Many counterfeit goods are produced and manufactured in China, making it the counterfeit capital of the world. In fact, the counterfeiting industry accounts for 8% of China's GDP. Counterfeit goods are produced and manufactured in Russia, North Korea, Taiwan, Bulgaria, and Greece as well. Greece is responsible for 2% of counterfeit goods seized by the EU. Some counterfeits are produced in the same factory that produces the original, authentic product, using inferior materials.

Another trend in counterfeiting, especially seen in consumer electronics, is the manufacture of entirely new products using poor quality materials or, more often, incorporating desirable features not present in a brand's authentic product line and then including prominent and fake brand names and logotypes to profit from brand recognition or brand image. An example would be imitation "Nokia" and "iPhone" cellular phones with features like dual SIM slots or analog TV, which are unavailable in authentic originals, or cosmetically-identical clones of high-end smartphones such as those from Hong Kong-based Goophone, using off the shelf system-on-chips from MediaTek and the Android operating system, often with user interfaces made to resemble the devices they imitate. Another example would be imitation "iPod" MP3 players whose batteries are removable and replaceable, whereas in authentic originals the batteries are permanently installed.

In the United States, a federal crackdown on counterfeit imports is driving an increase in domestic output of fake merchandise, according to investigators and industry executives. Raids carried out in New York City resulted in the seizure of an estimated $200 Million in counterfeit apparel, bearing the logos of brands such as "The North Face," "Polo," "Izod Lacoste," "Rocawear," "Seven for all Mankind," and "Fubu." One of the largest seizures was a joint operation in Arizona, Texas and California that seized seventy-seven containers of fake "Nike Air Jordan" shoes and a container of "Abercrombie & Fitch" clothing, valued at $69.5 million. Another current method of attacking counterfeits is at the retail level. Fendi sued the Sam's Club division of Walmart for selling fake "Fendi" bags and leather goods in five states. Sam's Club agreed to pay Fendi a confidential amount to settle the dispute and dismiss the action.

In the case *Tiffany v. eBay*, Tiffany & Co. sued auction site eBay for allowing the sale of counterfeit items, but lost on all claims. Gucci filed suit against thirty websites in the United States and is currently in the process of suing one hundred more.

A number of companies involved in the development of anti-counterfeiting and brand protection solutions have come together to form special industry-wide and global organisations dedicated to combating the so-called "brand pirates" such as the International Hologram Manufacturers Association. Other companies and organisations have established web-based communities that provide a framework for crowd-sourced solutions to counterfeiting. One such free community, Collectors Proof enables manufacturers and users alike to associate unique identification numbers to virtually any item so that each new owner can update its chain of custody. Because quality counterfeit items are often difficult to discern from authentic goods, this approach enables potential customers to access an item's current and previous owners – its provenance – prior to purchase.

To combat counterfeiting, companies may have the various parts of an item manufactured in independent factories and then limit the supply of certain distinguishing parts to the factory that performs the final assembly to the exact number required for the number of items to be assembled (or as near to that number as is practicable) or may require the factory to account for every part used and to return any unused, faulty or damaged parts. To help distinguish the originals from the counterfeits, the copyright holder may also employ the use of serial numbers or holograms etc., which may be attached to the product in another factory still.

Forgery

Forgery is the process of making, adapting, or imitating objects, statistics, or documents with the intent to deceive for the sake of altering the public perception, or to earn profit by selling the forged item. Copies, studio replicas, and reproductions are not considered forgeries, though they may later become forgeries through knowing and willful misrepresentations. Forging money or currency is more often called counterfeiting. But consumer goods may also be *counterfeits* if they are not manufactured or produced by the designated manufacturer or producer given on the label or flagged by the trademark symbol. When the object forged is a record or document it is often called a false document.

This usage of "forgery" does not derive from metalwork done at a forge, but it has a parallel history. A sense of "to counterfeit" is already in the Anglo-French verb *forger*, meaning "falsify".

A forgery is essentially concerned with a produced or altered object. Where the prime concern of a forgery is less focused on the object itself – what it is worth or what it "proves" – than on a tacit statement of criticism that is revealed by the reactions the object provokes in others, then the larger process is a hoax. In a hoax, a rumor or a genuine object planted in a concocted situation, may substitute for a forged physical object.

The similar crime of fraud is the crime of deceiving another, including through the use of objects obtained through forgery. Forgery is one of the techniques of fraud, including identity theft. Forgery is one of the threats addressed by security engineering.

In the 16th century, imitators of Albrecht Dürer's style of printmaking improved the market for their own prints by signing them "AD", making them forgeries. In the 20th century the art market made forgeries highly profitable. There are widespread forgeries of especially valued artists, such as drawings originally by Pablo Picasso, Paul Klee, and Henri Matisse.

A special case of double forgery is the forging of Vermeer's paintings by Han van Meegeren, and in its turn the forging of Van Meegeren's work by his son Jacques van Meegeren.

England and Wales and Northern Ireland

In England and Wales and Northern Ireland, forgery is an offence under section 1 of the Forgery and Counterfeiting Act 1981, which provides:

A person is guilty of forgery if he makes a false instrument, with the intention that he or another shall use it to induce somebody to accept it as genuine, and by reason of so accepting it to do or not to do some act to his own or any other person's prejudice.

"Instrument" is defined by section 8, "makes" and "false" by section 9, and "induce" and "prejudice" by section 10.

Forgery is triable either way. A person guilty of forgery is liable, on conviction on indictment, to imprisonment for a term not exceeding ten years, or, on summary conviction, to imprisonment for a term not exceeding six months, or to a fine not exceeding the statutory maximum, or to both.

The common law offence of forgery is abolished for all purposes not relating to offences committed before the commencement of the Forgery and Counterfeiting Act 1981.

Scotland

Forgery is not an official offence under the law of Scotland, except in cases where statute provides otherwise.

The Forgery of Foreign Bills Act 1803 was repealed in 2013.

Republic of Ireland

In the Republic of Ireland, forgery is an offence under section 25(1) of the Criminal Justice (Theft and Fraud Offences) Act, 2001 which provides:

A person is guilty of forgery if he or she makes a false instrument with the intention that it shall be used to induce another person to accept it as genuine and, by reason of so accepting it, to do some act, or to make some omission, to the prejudice of that person or any other person.

A person guilty of forgery is liable, on conviction on indictment, to imprisonment for a term not exceeding ten years, or to a fine, or to both.

Any offence at common law of forgery is abolished. The abolition of a common law offence of forgery does not affect proceedings for any such offence committed before its abolition.

Except as regards offences committed before the commencement of the Criminal Justice (Theft and Fraud Offences) Act, 2001 and except where the context otherwise requires, without prejudice to section 65(4)(a) of that Act, references to forgery must be construed in accordance with the provisions of that Act.

Canada

Forgery is an offence under sections 366, 367 and 368 of the Canadian Criminal Code. The offence is a hybrid offence, subject to a maximum prison sentence of:

- if tried summarily: 6 months
- if tried on indictment: 10 years

United States

Forgery is a crime in all jurisdictions within the United States, including state and federal. Most states, including California, describe forgery as occurring when a person alters a written document "with the intent to defraud, knowing that he or she has no authority to do so." The written document usually has to be an instrument of legal significance. Punishments for forgery vary widely. In California, forgery for an amount under $950 can result in misdemeanor charges and no jail time, while a forgery involving a loss of over $500,000 can result in three years in prison for the forgery plus a five-year "conduct enhancement" for the amount of the loss, yielding eight years in prison. In Connecticut, forgery in the Third Degree, which is a class B misdemeanor is punishable by up to 6 months in jail, a $1000 fine, and probation; forgery in the First Degree, which is a class C felony , is punishable by a maximum 10 years in prison, a fine of up to $10,000 fine, or both.

Civil law

As to the effect, in the United Kingdom, of a forged signature on a bill of exchange, see section 24 of the Bills of Exchange Act 1882.

Documentary art

Before the invention of photography, people commonly hired painters and engravers to "re-create" an event or a scene. Artists had to imagine what to illustrate based on the information available to them about the subject. Some artists added elements to

make the scene more exotic, while others removed elements out of modesty. In the 18th century, for example, Europeans were curious about what North America looked like and were ready to pay to see illustrations depicting this faraway place. Some of these artists produced prints depicting North America, despite many having never left Europe.

In popular culture

- The 1839 novel by Honoré de Balzac, *Pierre Grassou*, concerns an artist who lives off forgeries.
- The Orson Welles documentary *F for Fake* concerns both art and literary forgery. For the movie, Welles intercut footage of Elmyr de Hory, an art forger, and Clifford Irving, who wrote an "authorized" autobiography of Howard Hughes that had been revealed to be a hoax. While forgery is the ostensible subject of the film, it also concerns art, film making, storytelling and the creative process.
- The 1966 heist comedy film *How to Steal a Million* centers around Nicole Bonnet (Audrey Hepburn) attempting to steal a fake Cellini made by her grandfather.
- The 1972 novel by Irving Wallace, *The Word* concerns archaeological forgery, the finding and translation of a supposed lost gospel by James the Just, close relative of Jesus Christ, as part of a large project to be published as a new Bible that would inspire a Christian revival, but which is possibly a forged document.
- The 2002 film *Catch Me If You Can*, directed by Steven Spielberg, is based on the real story of Frank Abagnale, a con man who stole over $2.5 million through forgery, imposture and other frauds, which are dramatized in the film. His career in crime lasted six years from 1963 to 1969.
- The graphic art novel *The Last Coiner*, authored by Peter M. Kershaw, is based on the exploits of the 18th century counterfeiters, the Cragg Vale Coiners, who were sentenced to execution by hanging at Tyburn.

Insider trading

Insider trading is the trading of a public company's stock or other securities (such as bonds or stock options) by individuals with access to nonpublic information about the company. In various countries, some kinds of trading based on insider information is illegal. This is because it is seen as unfair to other investors who do not have access to the information, as the investor with insider information could potentially make larger profits than a typical investor could make.

The authors of one study claim that illegal insider trading raises the cost of capital for securities issuers, thus decreasing overall economic growth. However, some economists, such as Henry Manne, have argued that insider trading should be allowed and could, in fact, benefit markets.

Trading by specific insiders, such as employees, is commonly permitted as long as it does not rely on material information not in the public domain. Many jurisdictions require that such trading be reported so that the transactions can be monitored. In the United States and several other jurisdictions, trading conducted by corporate officers, key employees, directors, or significant shareholders must be reported to the regulator or publicly disclosed, usually within a few business days of the trade. In these cases, insiders in the United States are required to file a Form 4 with the U.S. Securities and Exchange Commission(SEC) when buying or selling shares of their own companies.

The rules governing insider trading are complex and vary significantly from country to country. The extent of enforcement also varies from one country to another. The definition of insider in one jurisdiction can be broad, and may cover not only insiders themselves but also any persons related to them, such as brokers, associates and even family members. A person who becomes aware of non-public informationand trades on that basis may be guilty of a crime.

Illegal

Rules prohibiting or criminalizing insider trading on material non-public information exist in most jurisdictions around the world (Bhattacharya and Daouk, 2002), but the details and the efforts to enforce them vary considerably. In the United States, Sections 16(b) and 10(b) of the Securities Exchange Act of 1934 directly and indirectly address insider trading. The U.S. Congress enacted this law after the stock market crash of 1929. While the United States is generally viewed as making the most serious efforts to enforce its insider trading laws, the broader scope of the European

model legislation provides a stricter framework against illegal insider trading. In the European Union and the United Kingdom all trading on non-public information is, under the rubric of market abuse, subject at a minimum to civil penalties and to possible criminal penalties as well. UK's Financial Conduct Authority has the responsibility to investigate and prosecute insider dealing, defined by The Criminal Justice Act 1993.

Definition of "insider"

In the United States, Canada, Australia and Germany, for mandatory reporting purposes, corporate insiders are defined as a company's officers, directors and any beneficial owners of more than 10% of a class of the company's equity securities. Trades made by these types of insiders in the company's own stock, based on material non-public information, are considered fraudulent since the insiders are violating the fiduciary duty that they owe to the shareholders. The corporate insider, simply by accepting employment, has undertaken a legal obligation to the shareholders to put the shareholders' interests before their own, in matters related to the corporation. When insiders buy or sell based upon company-owned information, they are violating their obligation to the shareholders.

For example, illegal insider trading would occur if the chief executive officer of Company A learned (prior to a public announcement) that Company A will be taken over and then bought shares in Company A while knowing that the share price would likely rise.

In the United States and many other jurisdictions, however, "insiders" are not just limited to corporate officials and major shareholders where illegal insider trading is concerned but can include any individual who trades shares based on material non-public information in violation of some duty of trust. This duty may be imputed; for example, in many jurisdictions, in cases of where a corporate insider "tips" a friend about non-public information likely to have an effect on the company's share price, the duty the corporate insider owes the company is now imputed to the friend and the friend violates a duty to the company if he trades on the basis of this information.

Liability

Liability for inside trading violations generally cannot be avoided by passing on the information in an "I scratch your back; you scratch mine" or quid pro quo arrangement if the person receiving the information knew or should have known that the information was material non-public information. In the United States, at least one court has indicated that the insider who releases the non-public information must have done so for an improper purpose. In the case of a person who receives the insider

information (called the "tippee"), the tippee must also have been aware that the insider released the information for an improper purpose.

One commentator has argued that if Company A's CEO did not trade on the undisclosed takeover news, but instead passed the information on to his brother-in-law who traded on it, illegal insider trading would still have occurred (albeit by proxy by passing it on to a "non-insider" so Company A's CEO would not get his hands dirty).

Misappropriation theory

A newer view of insider trading, the misappropriation theory, is now accepted in U.S. law. It states that anyone who misappropriates information from his or her employer and trades on that information in **any**stock (either the employer's stock or the company's competitor stocks) may be guilty of insider trading.

Proof of responsibility

Proving that someone has been responsible for a trade can be difficult because traders may try to hide behind nominees, offshore companies, and other proxies.
The Securities and Exchange Commissionprosecutes over 50 cases each year, with many being settled administratively out of court. The SEC and several stock exchanges actively monitor trading, looking for suspicious activity. The SEC does not have criminal enforcement authority, but can refer serious matters to the U.S. Attorney's Office for further investigation and prosecution.

Trading on information in general

In the United States and most non-European jurisdictions not all trading on non-public information is illegal insider trading. For example, a person in a restaurant who hears the CEO of Company A at the next table tell the CFO that the company's profits will be higher than expected and then buys the stock is not guilty of insider trading—unless he or she had some closer connection to the company or company officers. However, even where the tippee is not himself an insider, where the tippee knows that the information is non-public and the information is paid for, or the tipper receives a benefit for giving it, then in the broader-scope jurisdictions the subsequent trading is illegal.

Notwithstanding, information about a tender offer (usually regarding a merger or acquisition) is held to a higher standard. If this type of information is obtained (directly or indirectly) and there is reason to believe it is nonpublic, there is a duty to disclose it or abstain from trading.

The punishment for insider trading depends on a few different factors. There are three main factors, which can be identified. Depending on jurisdictions, there may be either civil or criminal penalties, or both.

- Scope – How many people were affected by the wrongdoing?
- Gain – How much did the insider make from the transaction, whether directly or as a tipster? Where there is a tipster and a tippee, how much did the tippee make from the transaction?
- Evidence – Anyone charged is innocent until proven guilty. The burden of proof falls on the prosecution. If no one "flips," or if there is no smoking gun, the prosecution has a harder time proving guilt. This may result in prosecution moving away from criminal charges, and instead choosing to pursue civil charges.

In the United States in addition to civil penalties, the trader may also be subject to criminal prosecution for fraud or where SEC regulations have been broken, the U.S. Department of Justice (DOJ) may be called to conduct an independent parallel investigation. If the DOJ finds criminal wrongdoing, the Department may file criminal charges.

Tracking

Since insiders are required to report their trades, others often track these traders, and there is a school of investing which follows the lead of insiders. Following such leads subjects the follower to the risk that an insider is making a buy specifically to increase investor confidence, or is making a sale for reasons unrelated to the health of the company (such as a desire to diversify or pay a personal expense).

Legal

Legal trades by insiders are common, as employees of publicly traded corporations often have stock or stock options. These trades are made public in the United States through Securities and Exchange Commission filings, mainly Form 4.

U.S. SEC Rule 10b5-1 clarified that the prohibition against insider trading does not require proof that an insider actually used material nonpublic information when conducting a trade; possession of such information alone is sufficient to violate the provision, and the SEC would infer that an insider in possession of material nonpublic information used this information when conducting a trade. However, SEC Rule 10b5-1 also created for insiders an affirmative defense if the insider can demonstrate

that the trades conducted on behalf of the insider were conducted as part of a pre-existing contract or written binding plan for trading in the future.

For example, if an insider expects to retire after a specific period of time and, as part of retirement planning, the insider has adopted a written binding plan to sell a specific amount of the company's stock every month for two years, and the insider later comes into possession of material nonpublic information about the company, trades based on the original plan might not constitute prohibited insider trading.

American law

Until the 21st Century and the European Union's market abuse laws, the United States was the leading country in prohibiting insider trading made on the basis of material non-public information. Thomas Newkirk and Melissa Robertson of the U.S. Securities and Exchange Commission (SEC) summarize the development of US insider trading laws. Insider trading has a base offense level of 8, which puts it in Zone A under the U.S. Sentencing Guidelines. This means that first-time offenders are eligible to receive probation rather than incarceration.

Statutory

U.S. insider trading prohibitions are based on English and American common law prohibitions against fraud. In 1909, well before the Securities Exchange Act was passed, the United States Supreme Court ruled that a corporate director who bought that company's stock when he knew the stock's price was about to increase committed fraud by buying but not disclosing his inside information.

Section 15 of the Securities Act of 1933 contained prohibitions of fraud in the sale of securities which were greatly strengthened by the Securities Exchange Act of 1934.

Section 16(b) of the Securities Exchange Act of 1934 prohibits short-swing profits (from any purchases and sales within any six-month period) made by corporate directors, officers, or stockholders owning more than 10% of a firm's shares. Under Section 10(b) of the 1934 Act, SEC Rule 10b-5, prohibits fraud related to securities trading.

The Insider Trading Sanctions Act of 1984 and the Insider Trading and Securities Fraud Enforcement Act of 1988 place penalties for illegal insider trading as high as three times the amount of profit gained or loss avoided from the illegal trading.

SEC regulations

SEC regulation FD ("Fair Disclosure") requires that if a company intentionally discloses material non-public information to one person, it must simultaneously disclose that information to the public at large. In the case of an unintentional disclosure of material non-public information to one person, the company must make a public disclosure "promptly."

Insider trading, or similar practices, are also regulated by the SEC under its rules on takeovers and tender offers under the Williams Act.

Court decisions

Much of the development of insider trading law has resulted from court decisions.

In 1909, the Supreme Court of the United States ruled in *Strong v. Repide*that a director who expects to act in a way that affects the value of shares cannot use that knowledge to acquire shares from those who do not know of the expected action. Even though in general, ordinary relations between directors and shareholders in a business corporation are not of such a fiduciary nature as to make it the duty of a director to disclose to a shareholder the general knowledge which he may possess regarding the value of the shares of the company before he purchases any from a shareholder, yet there are cases where, by reason of the special facts, such duty exists.

In 1968, the Second Circuit Court of Appeals advanced a "level playing field" theory of insider trading in *SEC v. Texas Gulf Sulphur Co.* The court stated that anyone in possession of inside information must either disclose the information or refrain from trading. Officers of the Texas Gulf Sulphur Corporation had used inside information about the discovery of the Kidd Mine to make profits by buying shares and call options on company stock.

In 1984, the Supreme Court of the United States ruled in the case of *Dirks v. Securities and Exchange Commission* that tippees (receivers of second-hand information) are liable if they had reason to believe that the tipper had breached a fiduciary duty in disclosing confidential information. One such example would be if the tipper received any personal benefit from the disclosure, thereby breaching his or her duty of loyalty to the company. In *Dirks*, the "tippee" received confidential information from an insider, a former employee of a company. The reason the insider disclosed the information to the tippee, and the reason the tippee disclosed the information to third parties, was to blow the whistle on massive fraud at the company. As a result of the tippee's efforts the fraud was uncovered, and the company went into bankruptcy. But, while the tippee had given the "inside" information to clients who

made profits from the information, the U.S. Supreme Court ruled that the tippee could not be held liable under the federal securities laws—for the simple reason that the insider from whom he received the information was not releasing the information for an improper purpose (a personal benefit), but rather for the purpose of exposing the fraud. The Supreme Court ruled that the tippee could not have been aiding and abetting a securities law violation committed by the insider—for the simple reason that no securities law violation had been committed by the insider.

In *Dirks*, the Supreme Court also defined the concept of "constructive insiders," who are lawyers, investment bankers and others who receive confidential information from a corporation while providing services to the corporation. Constructive insiders are also liable for insider trading violations if the corporation expects the information to remain confidential, since they acquire the fiduciary duties of the true insider.

The next expansion of insider trading liability came in *SEC vs. Materia* 745 F.2d 197 (2d Cir. 1984), the case which first introduced the misappropriation theory of liability for insider trading. Materia, a financial printing firm proofreader, and clearly not an insider by any definition, was found to have determined the identity of takeover targets based on proofreading tender offer documents during his employment. After a two-week trial, the district court found him liable for insider trading, and the Second Circuit Court of Appeals affirmed holding that the theft of information from an employer, and the use of that information to purchase or sell securities in another entity, constituted a fraud in connection with the purchase or sale of a securities. The misappropriation theory of insider trading was born, and liability further expanded to encompass a larger group of outsiders.

In *United States v. Carpenter* (1986) the U.S. Supreme Court cited an earlier ruling while unanimously upholding mail and wire fraud convictions for a defendant who received his information from a journalist rather than from the company itself. The journalist R. Foster Winans was also convicted, on the grounds that he had misappropriated information belonging to his employer, the *Wall Street Journal*. In that widely publicized case, Winans traded in advance of "Heard on the Street" columns appearing in the Journal.

The Court stated in *Carpenter*: "It is well established, as a general proposition, that a person who acquires special knowledge or information by virtue of a confidential or fiduciary relationship with another is not free to exploit that knowledge or information for his own personal benefit but must account to his principal for any profits derived therefrom."

However, in upholding the securities fraud (insider trading) convictions, the justices were evenly split.

In 1997, the U.S. Supreme Court adopted the misappropriation theory of insider trading in *United States v. O'Hagan*, 521 U.S. 642, 655 (1997). O'Hagan was a partner in a law firm representing Grand Metropolitan, while it was considering a tender offer for Pillsbury Company. O'Hagan used this inside information by buying call options on Pillsbury stock, resulting in profits of over $4.3 million. O'Hagan claimed that neither he nor his firm owed a fiduciary duty to Pillsbury, so he did not commit fraud by purchasing Pillsbury options.

The Court rejected O'Hagan's arguments and upheld his conviction.

The "misappropriation theory" holds that a person commits fraud "in connection with" a securities transaction and thereby violates 10(b) and Rule 10b-5, when he misappropriates confidential information for securities trading purposes, in breach of a duty owed to the source of the information. Under this theory, a fiduciary's undisclosed, self-serving use of a principal's information to purchase or sell securities, in breach of a duty of loyalty and confidentiality, defrauds the principal of the exclusive use of the information. In lieu of premising liability on a fiduciary relationship between company insider and purchaser or seller of the company's stock, the misappropriation theory premises liability on a fiduciary-turned-trader's deception of those who entrusted him with access to confidential information.

The Court specifically recognized that a corporation's information is its property: "A company's confidential information ... qualifies as property to which the company has a right of exclusive use. The undisclosed misappropriation of such information in violation of a fiduciary duty ... constitutes fraud akin to embezzlement – the fraudulent appropriation to one's own use of the money or goods entrusted to one's care by another."

In 2000, the SEC enacted SEC Rule 10b5-1, which defined trading "on the basis of" inside information as any time a person trades while aware of material nonpublic information. It is no longer a defense for one to say that one would have made the trade anyway. The rule also created an affirmative defense for pre-planned trades.

In 2014, in the case of *United States v. Newman*, the United States Court of Appeals for the Second Circuit cited the Supreme Court's decision in *Dirks*, and ruled that in order for a "tippee" (a person who has received insider information from an insider and has used that information) to be guilty of insider trading, the tippee must have been aware not only that the information was insider information, but must also have been aware that the insider released the information for an improper purpose (such as a personal benefit). The Court concluded that the insider's breach of a fiduciary duty not to release confidential information—in the absence of an improper purpose on the

part of the insider—is not enough for criminal liability to be imposed on the either the insider or the tippee.

In 2016, in the case of *Salman v. United States*, the U.S. Supreme Court held that the benefit a tipper has to receive as predicate for an insider-trader prosecution of a tippee need not be pecuniary, and that giving a 'gift' of a tip to a family member is presumptively an act for the personal though intangible benefit of the tipper.

By members of Congress

Members of the US Congress are not exempt from the laws that ban insider trading. Because they generally do not have a confidential relationship with the source of the information they receive, however, they do not meet the usual definition of an "insider." House of Representatives rules may however consider congressional insider trading unethical. A 2004 study found that stock sales and purchases by Senators outperformed the market by 12.3% per year. Peter Schweizer points out several examples of insider trading by members of Congress, including action taken by Spencer Bachus following a private, behind-the-doors meeting on the evening of September 18, 2008 when Hank Paulson and Ben Bernanke informed members of Congress about the imminent financial crisis, Bachus then shorted stocks the next morning and cashed in his profits within a week. Also attending the same meeting were Senator Dick Durbin and John Boehner; the same day (trade effective the next day), Durbin sold mutual-fund shares worth $42,696, and reinvested it all with Warren Buffett. Also the same day (trade effective the next day), Congressman Boehner cashed out of an equity mutual fund.

In May 2007, a bill entitled the "Stop Trading on Congressional Knowledge Act, or STOCK Act" was introduced that would hold congressional and federal employees liable for stock trades they made using information they gained through their jobs and also regulate analysts or "Political Intelligence" firms that research government activities. The 2012 STOCK Act was passed on April 4, 2012.

With congress-sourced information

In 2014, federal prosecutors issued a subpoena to the House Ways and Means committee and Brian Sutter, staff director of its health-care sub-committee, relative to a price move in stocks just prior to the passage of a law favorable to the companies involved. An e-mail was sent out by a "Washington-based policy-research firm that predicted the change [in the law] for its Wall Street clients. That alert, in turn, was based in part on information provided to the firm by a former congressional health-care aide turned lobbyist, according to emails reviewed by the *[Wall Street] Journal* in 2013.

Security analysis

Security analysts gather and compile information, talk to corporate officers and other insiders, and issue recommendations to traders. Thus their activities may easily cross legal lines if they are not especially careful. The CFA Institute in its code of ethics states that analysts should make every effort to make all reports available to all the broker's clients on a timely basis. Analysts should never report material nonpublic information, except in an effort to make that information available to the general public. Nevertheless, analysts' reports may contain a variety of information that is "pieced together" without violating insider trading laws, under the Mosaic theory. This information may include non-material nonpublic information as well as material public information, which may increase in value when properly compiled and documented.

Arguments for legalizing

Some economists and legal scholars (such as Henry Manne, Milton Friedman, Thomas Sowell, Daniel Fischel, and Frank H. Easterbrook) have argued that laws against insider trading should be repealed. They claim that insider trading based on material nonpublic information benefits investors, in general, by more quickly introducing new information into the market.

Friedmann, laureate of the Nobel Memorial Prize in Economics, said: "You want more insider trading, not less. You want to give the people most likely to have knowledge about deficiencies of the company an incentive to make the public aware of that." Friedman did not believe that the trader should be required to make his trade known to the public, because the buying or selling pressure itself is information for the market.

Other critics argue that insider trading is a victimless act: a willing buyer and a willing seller agree to trade property which the seller rightfully owns, with no prior contract (according to this view) having been made between the parties to refrain from trading if there is asymmetric information. The Atlantic has described the process as "arguably the closest thing that modern finance has to a victimless crime".

Legalization advocates also question why "trading" where one party has more information than the other is legal in other markets, such as real estate, but not in the stock market. For example, if a geologistknows there is a high likelihood of the discovery of petroleum under Farmer Smith's land, he may be entitled to make Smith an offer for the land, and buy it, without first telling Farmer Smith of the geological data. Nevertheless, circumstances can occur when the geologist would be committing fraud if, because he owes a duty to the farmer, he did not disclose the

information (for example, where the geologist had been hired by Farmer Smith to assess the geology of the farm).

Advocates of legalization make free speech arguments. Punishment for communicating about a development pertinent to the next day's stock price might seem an act of censorship. If the information being conveyed is proprietary information and the corporate insider has contracted to not expose it, he has no more right to communicate it than he would to tell others about the company's confidential new product designs, formulas, or bank account passwords.

Some authors have used these arguments to propose legalizing insider trading on negative information (but not on positive information). Since negative information is often withheld from the market, trading on such information has a higher value for the market than trading on positive information.

There are very limited laws against "insider trading" in the commodities markets if, for no other reason than that the concept of an "insider" is not immediately analogous to commodities themselves (corn, wheat, steel, etc.). However, analogous activities such as front running are illegal under US commodity and futures trading laws. For example, a commodity broker can be charged with fraud by receiving a large purchase order from a client (one likely to affect the price of that commodity) and then purchasing that commodity before executing the client's order to benefit from the anticipated price increase.

Commercialisation

The advent of the Internet has provided a forum for the commercialisation of trading on insider information. In 2016 a number of dark web sites were identified as marketplaces where such non-public information was bought and sold. At least one such site used bitcoins to avoid currency restrictions and to impede tracking. Such sites also provide a place for soliciting for corporate informants, where non-public information may be used for purposes other than stock trading.

Legal differences among jurisdictions

The US and the UK vary in the way the law is interpreted and applied with regard to insider trading. In the UK, the relevant laws are the Criminal Justice Act 1993, Part V, Schedule 1; the Financial Services and Markets Act 2000, which defines an offence of "Market Abuse"; and the European Union Regulation No 596/2014. The principle is that it is illegal to trade on the basis of market-sensitive information that is not generally known. This is a much broader scope that under U.S. law. The key differences from U.S. law are that no relationship to either the issuer of the security or

the tipster is required; all that is required is that the guilty party traded (or caused trading) whilst having inside information, and there is no scienter requirement under UK law.

Japan enacted its first law against insider trading in 1988. Roderick Seeman said, "Even today many Japanese do not understand why this is illegal. Indeed, previously it was regarded as common sense to make a profit from your knowledge."

In Malta the law follows the European broader scope model. The relevant statute is the Prevention of Financial Markets Abuse Act of 2005, as amended. Earlier acts included the Financial Markets Abuse Act in 2002, and the Insider Dealing and Market Abuse Act of 1994.

The International Organization of Securities Commissions (IOSCO) paper on the "Objectives and Principles of Securities Regulation" (updated to 2003) states that the three objectives of good securities market regulation are:

1. Investor protection,
2. Insuring that markets are fair, efficient and transparent, and
3. Reducing systemic risk.

The discussion of these "Core Principles" state that "investor protection" in this context means "Investors should be protected from misleading, manipulative or fraudulent practices, including insider trading, front running or trading ahead of customers and the misuse of client assets." More than 85 percent of the world's securities and commodities market regulators are members of IOSCO and have signed on to these Core Principles.

The World Bank and International Monetary Fund now use the IOSCO Core Principles in reviewing the financial health of different country's regulatory systems as part of these organization's financial sector assessment program, so laws against insider trading based on non-public information are now expected by the international community. Enforcement of insider trading laws varies widely from country to country, but the vast majority of jurisdictions now outlaw the practice, at least in principle.

Larry Harris claims that differences in the effectiveness with which countries restrict insider trading help to explain the differences in executive compensation among those countries. The US, for example, has much higher CEO salaries than do Japan or Germany, where insider trading is less effectively restrained.

By nation

European Union

In 2014, the European Union (EU) adopted legislation (Criminal Sanctions for Market Abuse Directive) that harmonises criminal sanctions for insider dealing. All EU Member States agreed to introduce maximum prison sentences of at least four years for serious cases of market manipulation and insider dealing, and at least two years for improper disclosure of insider information.

Norway

In 2009, a journalist in Nettavisen (Thomas Gulbrandsen) was sentenced to 4 months in prison for insider trading.

The longest prison sentence in a Norwegian trial where the main charge was insider trading, was for 8 years (2 of which suspended) when Alain Angelil was convicted in a district court on December 9, 2011.

United Kingdom

Although insider trading in the UK has been illegal since 1980, it proved difficult to successfully prosecute individuals accused of insider trading. There were a number of notorious cases where individuals were able to escape prosecution. Instead the UK regulators relied on a series of fines to punish market abuses.

These fines were widely perceived as an ineffective deterrent (Cole, 2007), and there was a statement of intent by the UK regulator (the Financial Services Authority) to use its powers to enforce the legislation (specifically the Financial Services and Markets Act 2000). Between 2009–2012 the FSA secured 14 convictions in relation to insider dealing.

United States

Rajat Gupta, who had been managing partner of McKinsey & Co. and a director at Goldman Sachs Group Inc. and Procter & Gamble Co., was convicted by a federal jury in 2012 of leaking inside information to hedge fund manager Raj Rajaratnam. The case was prosecuted by the office of United States Attorney for the Southern District of New York Preet Bharara.

With the guilty plea by Perkins Hixon in 2014 for insider trading from 2010-2013 while at Evercore Partners, Bharara said in a press release that 250 defendants whom his office had charged since August 2009 had now been convicted.

On December 10, 2014, a federal appeals court overturned the insider trading convictions of two former hedge fund traders, Todd Newman and Anthony Chiasson, based on the "erroneous" instructions given to jurors by the trial judge. The decision was expected to affect the appeal of the separate insider-trading conviction of former SAC Capital portfolio manager Michael Steinberg and the U.S. Attorney and the SEC in 2015 did drop their cases against Steinberg and others.

In 2016, Sean Stewart, a former managing director at Perella Weinberg Partners LP and vice president at JPMorgan Chase, was convicted on allegations he tipped his father on pending health-care deals. The father, Robert Stewart, previously had pleaded guilty but didn't testify during his son's trial. It was argued that by way of compensation for the tip, the father had paid more than $10,000 for Sean's wedding photographer.

In 2017, Billy Walters, Las Vegas sports bettor, was convicted of making $40 million on private information of Dallas-based dairy processing company Dean Foods. Walters's source, company director Thomas C. Davis employing a prepaid cell phone and sometimes the code words "Dallas Cowboys" for Dean Foods, helped him from 2008 to 2014 realize profits and avoid losses in the stock, the Federal jury found. In the trial, investor Carl C. Icahn was mentioned in relation to Walters's trading but was not charged with wrongdoing. Golfer Phil Mickelson "was also mentioned during the trial as someone who had traded in Dean Foods shares and once owed nearly $2 million in gambling debts to" Walters. Mickelson "made roughly $1 million trading Dean Foods shares; he agreed to forfeit those profits in a related civil case brought by the Securities and Exchange Commission". Walters's lawyer said he would appeal the verdict.

Canada

In 2008, police uncovered an insider trading conspiracy involving Bay Street and Wall Street lawyer Gil Cornblum and another lawyer, Stan Grmovsek, who were found to have gained over $10 million in illegal profits over a 14-year span. Cornblum committed suicide before criminal charges were laid. Grmovsek pleaded guilty and was sentenced to 39 months in prison. This was the longest term ever imposed for insider trading in Canada. These crimes were explored in Mark Coakley's 2011 non-fiction book, Tip and Trade.

China

On October 1, 2015, Chinese fund manager Xu Xiang was arrested due to insider trading.

India

Insider Trading in India is an offense according to Section 195 of the Companies Act, 2013 and Sections 12A, 15G of the Securities and Exchange Board of India Act, 1992. Insider trading is when one with access to non public, price sensitive information about the securities of the company subscribes, buys, sells or deals, or agrees to do so or counsels another to do as principal or agent. Price sensitive information is information that will materially affect the value of the securities. The penalty for insider trading is imprisonment, which may extend to five years, and a minimum of five lakh rupees (five hundred thousand) to twenty five crore rupees (two hundred and fifty million) or three times the profit made; whichever is higher.

Standards for Legal Insider Trading

Insider trading is legal as long as disclosure of the holdings and trading in securities of the company is done by the insiders. Any other connected person or group of connected persons shall also disclose their holdings under this regulation.

The gist of these rules is that an insider cannot trade on non-public information until that information is disclosed, and cannot tip people off using non-public information.

SEBI Guidelines For Disclosures of Trading by Insiders

1. Promoters, key managerial personnel and director of every company whose securities are listed on any recognized exchange shall disclose his holding of securities within 30 days of these regulations taking effect to the company.

2. Every person on appointment as key managerial personnel, director of the company or upon becoming a promoter shall disclose his holding of securities of company within 7 days of such appointment to the company.

3. Every promoter, director or employee of the company shall disclose to the company, the number of securities acquired or disposed of within two days of such transaction, if the value of securities traded through one transaction or series of

transaction in a calendar quarter exceeds 10 lakh rupees or any other value as may be prescribed.

4. Company needs to inform within two days of receipt of such disclosure to the stock exchange.

5 Disclosure by the connected person shall be made as required by the company.

Philippines

Under Republic Act 8799 or the Securities Regulation Code, insider trading in the Philippines is illegal.

White-collar crime

White-collar crime refers to financially motivated nonviolent crime committed by business and government professionals. Within criminology, it was first defined by sociologist Edwin Sutherland in 1939 as "a crime committed by a person of respectability and high social status in the course of his occupation". Typical white-collar crimes could include fraud, bribery, Ponzi schemes, insider trading, labor racketeering, embezzlement, cybercrime, copyright infringement, money laundering, identity theft, and forgery.

Modern criminology generally rejects a limitation of the term by reference, rather classifies the type of crime and the topic:

- By the type of offense, e.g., property crime, economic crime, and other corporate crimes like environmental and health and safety law violations. Some crime is only possible because of the identity of the offender, e.g., transnational money laundering requires the participation of senior officers employed in banks. But the FBI has adopted the narrow approach, defining white-collar crime as "those illegal acts which are characterized by deceit, concealment, or violation of trust and which are not dependent upon the application or threat of physical force or violence" (1989, 3). While the true extent and cost of white-collar crime are unknown, the FBI and the Association of Certified Fraud Examiners estimate the annual cost to the United States to fall between $300 and $660 billion.
- By the type of offender, e.g., by social class or high socioeconomic status, the occupation of positions of trust or profession, or academic qualification, researching the motivations for criminal behavior, e.g., greed or fear of loss of face if economic difficulties become obvious. Shover and Wright (2000) point to the essential neutrality of a crime as enacted in a statute. It almost inevitably describes conduct in the abstract, not by reference to the character of the persons performing it. Thus, the only way that one crime differs from another is in the backgrounds and characteristics of its perpetrators.
- By organizational culture rather than the offender or offense which overlaps with organized crime. Appelbaum and Chambliss offer a twofold definition:
    - Occupational crime which occurs when crimes are committed to promote personal interests, say, by altering records and overcharging, or by the cheating of clients by professionals.
    - Organizational or corporate crime which occurs when corporate executives commit criminal acts to benefit their company by overcharging or price fixing, false advertising, etc.

The types of crime committed are a function of what is available to the potential offender. Thus, those employed in relatively unskilled environments and living in inner-city areas have fewer opportunities to exploit than those who work in situations where large financial transactions occur and live in areas where there is relative prosperity. Blue-collar crime tends to be more obvious and thus attracts more active police attention such as vandalism or shoplifting. In contrast, white-collar employees can incorporate legitimate and criminal behavior, thus making themselves less obvious when committing the crime. Therefore, blue-collar crime will more often use physical force, whereas in the corporate world, the identification of a victim is less obvious and the issue of reporting is complicated by a culture of commercial confidentiality to protect shareholder value. It is estimated that a great deal of white-collar crime is undetected or, if detected, it is not reported.

Corporate crime deals with the company as a whole. The crime benefits the investors or the individuals who are in high positions in the company or corporation. The relationship white-collar crime has with corporate crime is that they are similar because they both are involved within the business world. Their difference is that white-collar crime benefits the individual involved, and corporate crime benefits the company or the corporation.

One well-known insider trading case in the United States is the ImClone stock trading case. In December 2001, top-level executives sold their shares in ImClone Systems, a pharmaceutical company that manufactured an anti-cancer drug. The U.S. Securities and Exchange Commission investigated numerous top-level executives, as well as Martha Stewart, a friend of ImClone's former chief executive who had also sold her shares at the same time. The SEC reached a settlement in 2005.

The negotiation of agreements between a state and a corporation will be at a relatively senior level on both sides, this is almost exclusively a white-collar "situation" which offers the opportunity for crime. Although law enforcement claims to have prioritized white-collar crime, evidence shows that it continues to be a low priority.

When senior levels of a corporation engage in criminal activity using the company this is sometimes called control fraud.

Organized transnational crime is organized criminal activity that takes place across national jurisdictions, and with advances in transportation and information technology, law enforcement officials and policymakers have needed to respond to this form of crime on a global scale. Some examples include human trafficking, money laundering, drug smuggling, illegal arms dealing, terrorism, and cybercrime. Although it is impossible to precisely gauge transnational crime, the Millennium

Project, an international think tank, assembled statistics on several aspects of transnational crime in 2009:

- World illicit trade of almost $780 billion
- Counterfeiting and piracy of $300 billion to $1 trillion
- Global drug trade of $321 billion

Individuals may commit crime during employment or unemployment. The two most common forms are theft and fraud. Theft can be of varying degrees, from a pencil to furnishings to a car. Insider trading, the trading of stock by someone with access to publicly unavailable information, is a type of fraud.

In the modern world, there are a lot of nations which divide the crimes into some laws. "Crimes Related to Inducement of Foreign Aggression" is the crime of communicating with aliens secretly to cause foreign aggression or menace. "Crimes Related to Foreign Aggression" is the treason of cooperating with foreign aggression positively regardless of the national inside and outside. "Crimes Related to Insurrection" is the internal treason. Depending on a country, conspiracy is added to these.

In the United States, sentences for white-collar crimes may include a combination of imprisonment, fines, restitution, community service, disgorgement, probation, or other alternative punishment. These punishments grew harsher after the Jeffrey Skilling and Enron scandal, when the Sarbanes–Oxley Act of 2002 was passed by the United States Congress and signed into law by President George W. Bush, defining new crimes and increasing the penalties for crimes such as mail and wire fraud. In other countries, such as China, white-collar criminals can be given the death penalty. Certain countries like Canada consider the relationship between the parties to be a significant feature on sentence when there is a breach of trust component involved. Questions about sentencing disparity in white-collar crime continue to be debated. Although, white-collar crime poses a serious threat in today's society, it becomes extremely difficult to identify. The FBI, concerned with identifying this type of offense, collects annual statistical information on only three categories: fraud, counterfeiting/forgery, and embezzlement. All other types of white-collar crime are listed in an, "miscellaneous" category.

Financial Action Task Force on Money Laundering (FATF)

The Financial Action Task Force (on Money Laundering) **(**FATF**), also known by its French name,** *Groupe d'action financière* **(**GAFI**), is an intergovernmental organization founded in 1989 on the initiative of the G7 to develop policies to combat money laundering. In 2001 its mandate expanded to include terrorism financing. It monitors progress in implementing the FATF Recommendations through "peer reviews" ("mutual evaluations") of member countries. The FATF Secretariat is housed at the OECD headquarters in Paris.**

FATF was formed by the 1989 G7 Summit in Paris to combat the growing problem of money laundering. The task force was charged with studying money laundering trends, monitoring legislative, financial and law enforcement activities taken at the national and international level, reporting on compliance, and issuing recommendations and standards to combat money laundering. At the time of its formation, FATF had 16 members, which by 2016 had grown to 37.

In its first year, FATF issued a report containing forty recommendations to more effectively fight money laundering. These standards were revised in 2003 to reflect evolving patterns and techniques in money laundering.

The mandate of the organisation was expanded to include terrorist financing following the September 11 terror attacks in 2001.

The FATF's primary policies issued are the Forty Recommendations on money laundering from 1990 and the 9 Special Recommendations (SR) on Terrorism Financing (TF).

Together, the Forty Recommendation and Special Recommendations on Terrorism Financing set the international standard for anti-money laundering measures and combating the financing of terrorism and terrorist acts. They set out the principles for action and allow countries a measure of flexibility in implementing these principles according to their particular circumstances and constitutional frameworks. Both sets of FATF Recommendations are intended to be implemented at the national level through legislation and other legally binding measures.

The FATF completely revised the Forty Recommendations in 1996 and 2003. The 2003 Forty Recommendations require states, among other things, to:

- Implement relevant international conventions
- Criminalise money laundering and enable authorities to confiscate the proceeds of money laundering
- Implement customer due diligence (e.g., identity verification), record keeping and suspicious transaction reporting requirements for financial institutions and designated non-financial businesses and professions
- Establish a financial intelligence unit to receive and disseminate suspicious transaction reports, and
- Cooperate internationally in investigating and prosecuting money laundering

The FATF issued 8 Special Recommendations on Terrorism Financing in October 2001, following the September 11 terrorist attacks in the United States. Among the measures, “Special Recommendation VIII” (SR VIII) was targeted specifically at nonprofit organizations. This was followed by the International Best Practices Combating the Abuse of Non-Profit Organizations in 2002, released one month before the U.S. Department of Treasury’s Anti-Terrorist Financing Guidelines, and the Interpretive Note for SR VIII in 2006.

In February 2004 (Updated as of February 2009) the FATF published a reference document Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations. The 2009 Handbook for Countries and Assessors outlines criteria for evaluating whether FATF standards are achieved in participating countries. In February 2012, the FATF codified its recommendations and Interpretive Notes into one document that maintains SR VIII (renamed “Recommendation 8”), and also includes new rules on weapons of mass destruction, corruption and wire transfers .

In addition to FATF's "Forty plus Nine" Recommendations, in 2000 FATF issued a list of "Non-Cooperative Countries or Territories" (NCCTs), commonly called the FATF Blacklist. This was a list of 15 jurisdictions that, for one reason or another, FATF members believed were uncooperative with other jurisdictions in international efforts against money laundering (and, later, terrorism financing). Typically, this lack of cooperation manifested itself as an unwillingness or inability (frequently, a legal inability) to provide foreign law enforcement officials with information relating to bank account and brokerage records, and customer identification and beneficial owner information relating to such bank and brokerage accounts, shell company, and other financial vehicles commonly used in money laundering. As of October 2006, there are no Non-Cooperative Countries and Territories in the context of the NCCT initiative. However FATF issues updates as countries on High-risk and non-cooperative jurisdictions list have made significant improvements in standards and cooperation. The FATF also issues updates to identify additional jurisdictions that pose Money Laundering/Terrorist Financing risks.

The effect of the FATF Blacklist has been significant, and arguably has proven more important in international efforts against money laundering than has the FATF Recommendations. While, under international law, the FATF Blacklist carried with it no formal sanction, in reality, a jurisdiction placed on the FATF Blacklist often found itself under intense financial pressure.

Associate members

As of 2015 there are 8 associate members:

- Asia/Pacific Group on Money Laundering (APG)
- Caribbean Financial Action Task Force (CFATF)
- Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
- Eurasian Group (EAG)
- Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL)(formerly PC-R-EV)
- Financial Action Task Force of Latin America (GAFILAT), formerly The Financial Action Task Force on Money Laundering in South America (GAFISUD)
- Inter-Governmental Action Group against Money Laundering in West Africa (GIABA)
- Middle East and North Africa Financial Action Task Force (MENAFATF)

Observer members

As of 2015 twenty five international organisations including for example the International Monetary Fund, the UN with six expert groups and the World Bank are observer organisations. The FATF welcomed the Kingdom of Saudi Arabia as an observer to the FATF.

Operation Green Quest

Operation Green Quest was a U.S. interagency investigative unit formed in October 2001 after the September 11 attacks. Sponsored by the United States Customs Service, it was concerned with the surveillance and interdiction of terrorist financing sources. It was disbanded in June 2003 pursuant to an agreement between the Department of Homeland Security and the Department of Justice.

Led by the U.S. Customs Service, and included agents and analysts from the Internal Revenue Service (IRS), the Secret Service, the Bureau of Alcohol, Tobacco and Firearms (ATF), the Federal Bureau of Investigation (FBI), the Office of Foreign Assets Control (OFAC), the Financial Crimes Enforcement Network (FinCEN), the U.S. Postal Inspection Service, and the Naval Criminal Investigative Service. Federal prosecutors from the U.S. Justice Department's Criminal Division also formed an integral part of Operation Green Quest. The director of Operation Green Quest was a senior special agent from U.S. Customs and the deputy director is a senior special agent from the IRS.

According to Customs, by its fourth month of Operation Green Quest had initiated more than 300 probes into terrorist finances, seizing about $10.3m in smuggled US currency and $4.3m in other assets. Its work resulted in 21 searches, 12 arrests and four indictments.

Its most spectacular operation of was March 20, 2002 raid 19 interrelated business and non-profit entities in Herndon, VA associated with an umbrella corporation known as the SAAR Foundation. No arrests were made and no organizations were shut down, but over 500 boxes of files and computer files were confiscated, filling seven trucks. Finding no incriminating evidence, much of the confiscated material has been returned.

The raid raised concerns of unfair persecution within the American Muslim community, leading to an April 4, 2002 meeting in which several notable Muslim figures, including Palestinian-American financier and Republican organizer Talat M. Othman and Islamic Institute head Khaled Saffuri were received by Treasury Secretary Paul O'Neill as representatives of the Muslim-American community to voice complaints about the raid.

Operation Green Quest Disbanded

As a result of conflicts between the FBI and the Bureau of Immigration and Customs Enforcement (the successor agency to Customs), in May 2003 the Attorney General

and the Secretary of Homeland Security signed an agreement concerning terrorist financing investigations. In it, DHS acknowledged that the Department of Justice, through the FBI, was the lead agency in the fight against terrorist financing, and that any terrorist financing investigations would have to be conducted under the auspices of the FBI-led Joint Terrorism Task Force. DHS also agreed to disband Operation Green Quest by June of that year, and not to start any investigations into terrorism or terrorist financing without the permission of the FBI.

Tax haven

A **tax haven** is a jurisdiction that has a low rate of tax or does not levy a tax as well as offers some degree of secrecy. Definitions vary; some definitions focus purely on tax: for example, one widely cited academic paper describes a tax haven as a jurisdiction where particular taxes, such as an inheritance tax or income tax, are levied at a low rate or not at all. However other definitions refer to a state, country, or territory which maintains a system of financial secrecy, which enables foreign individuals to hide assets or income to avoid or reduce taxes in their home jurisdiction. "Secrecy jurisdiction" is sometimes used as an alternative to "tax haven" to emphasise the secrecy element, and a Financial Secrecy Index ranks jurisdictions according to their size and secrecy.

Earnings from income generated from real estate (i.e. by renting property owned in an offshore jurisdiction) can also be eliminated in this way. If taxes (if any) are paid in the tax haven jurisdiction, companies can avoid taxes in their home jurisdiction because the tax had already been paid in the lower tax rate jurisdiction. Some taxes (such as inheritance tax on the real estate, VAT on the initial purchase price of the real estate, or transfer tax, annual immovable property taxes, and municipal real estate taxes) cannot be avoided or reduced, as these are levied by the country the real estate where the property is located, and hence need to be paid just the same as any other resident of that country. The only thing that can be done is picking a country that has the smallest rates on these taxes (or even no such taxes at all) before buying any real estate.

Individuals or corporate entities may establish shell subsidiaries or move themselves to areas with reduced or no taxation levels relative to typical international taxation. This creates a situation of tax competition among jurisdictions. Different jurisdictions may be havens for different types of taxes, and for different categories of people or companies. Sovereign jurisdictions or self-governing territories under international law have the power to enact tax laws affecting their territories, unless limited by previous international treaties.

There are several definitions of tax havens. In 2002 *The Economist* adopted the description by Geoffrey Colin Powell (former economic adviser to Jersey): "What ... identifies an area as a tax haven is the existence of a composite tax structure established deliberately to take advantage of, and exploit, a worldwide demand for opportunities to engage in tax avoidance." *The Economist* points out that this definition would still exclude a number of jurisdictions traditionally thought of as tax havens. Similarly, an Australian journalist suggested that any country which modifies its tax laws to attract foreign capital could be considered a tax haven.

According to other definitions, the central feature of a haven is that its laws and other measures can be used to evade or avoid the tax laws or regulations of other jurisdictions. the U.S. Government Accountability Office in its December 2008 report on the use of tax havens by American corporations, was unable to find a satisfactory definition of a tax haven but regarded the following characteristics as indicative of it: no or nominal taxes; lack of effective exchange of tax information with foreign tax authorities; lack of transparency in the operation of legislative, legal or administrative provisions; no requirement for a substantive local presence; and self-promotion as an offshore financial center.

As of February 2008 the Organisation for Economic Co-operation and Development (OECD) identified three key factors in considering whether a jurisdiction is a tax haven:

- No or only nominal taxes – Tax havens impose no or only nominal taxes (generally or in special circumstances) and offer themselves, or are perceived to offer themselves, as a place to be used by non-residents to escape high taxes in their country of residence.
- Protection of personal financial information – Tax havens typically have laws or administrative practices under which businesses and individuals can benefit from strict rules and other protections against scrutiny by foreign tax authorities. This prevents the transmittance of information about taxpayers who are benefiting from the low tax jurisdiction.
- Lack of transparency – A lack of transparency in the operation of the legislative, legal or administrative provisions is another factor used to identify tax havens. The OECD is concerned that laws should be applied openly and consistently, and that information needed by foreign tax authorities to determine a taxpayer's situation is available. Lack of transparency in one country can make it difficult, if not impossible, for other tax authorities to apply their laws effectively. 'Secret rulings', negotiated tax rates, or other practices that fail to apply the law openly and consistently are examples of a lack of transparency. Limited regulatory supervision or a government's lack of legal access to financial records are contributing factors.

However, the OECD found that its definition caught certain aspects of its members' tax systems (some countries have low or zero taxes and ring fencing for certain favored groups). Its later work has focused on the single aspect of information exchange. This is generally thought to be an inadequate definition of a tax haven, but is politically expedient, because it includes the small tax havens (with little power in the international political arena) but exempts the powerful countries with tax haven aspects such as the US and UK.

In deciding whether or not a jurisdiction is a tax haven, the first factor to look at is whether there are no or nominal taxes. If this is the case, the other two factors—whether or not there is an exchange of information and transparency—must be analyzed. Having no or nominal taxes is not sufficient, by itself, to characterize a jurisdiction as a tax haven. The OECD recognizes that every jurisdiction has a right to determine whether to impose direct taxes and, if so, to determine the appropriate tax rate.

Corporations, to avoid or reduce overall taxation may use multiple types of tax havens. Three types of tax haven types form a *Dutch Sandwich*:

- Primary tax havens – the location where financial capital winds up. Subsidiary shell companies there have obtained rights to collect profits from corporate intellectual property (IP) by transfers from their parent.
- Semi-tax havens – locations that produce goods for sale primarily outside of their territorial boundaries and have flexible regulations to encourage job growth, such as free trade zones, territorial-only taxation, and similar inducements.
- Conduit tax havens – locations where income from sales, primarily made outside their boundaries, is collected, and then distributed. Semi-tax havens are reimbursed for actual product costs, perhaps with a commodity markup. The remaining profits are transferred to the primary tax haven, because it holds rights to profits due to the corporate IP. By matching outflow to income, they do not retain capital and their role, while crucial, remains invisible.

Large multinational corporations may have dozen of such entities in tax haven jurisdictions interacting with each other. Each haven can claim that it does not satisfy definitions that attempt to place all tax havens into a single class. Even increased transparency may not change the effectiveness of corporate tax avoidance.

While incomplete, and with the limitations discussed below, the available statistics nonetheless indicate that offshore banking is a very sizable activity.
The OECD estimated in 2007 that capital held offshore amounted to between $5 trillion and $7 trillion, making up approximately 6–8% of total global investments under management.

A more recent study by Gabriel Zucman of the London School of Economics estimated the amount of global cross-border wealth held in tax havens (including the Netherlands and Luxembourg as tax havens for this purpose) at US$7.6 trillion, of which US$2.46 trillion was held in Switzerland alone. The Tax Justice Network (an anti-tax haven pressure group) estimated in 2012 that capital held

offshore amounted to between $21 trillion and $32 trillion (between 24–32% of total global investments), although those estimates have been challenged.

In 2000, the International Monetary Fund calculated based on Bank for International Settlements data that for selected offshore financial centres, on-balance sheet cross-border assets held in offshore financial centres reached a level of $4.6 trillion at the end of June 1999 (about 50 percent of total cross-border assets). Of that $4.6 trillion, $0.9 trillion was held in the Caribbean, $1 trillion in Asia, and most of the remaining $2.7 trillion accounted for by the major international finance centres (IFCs), namely London, the U.S. IBFs, and the Japanese offshore market. The U.S. Department of Treasury estimated that in 2011 the Caribbean Banking Centers, which include Bahamas, Bermuda, Cayman Islands, Netherlands Antilles and Panama, held almost $2 trillion dollars in United States debt. Of this, approximately US$1.4 trillion is estimated to be held in the Cayman Islands alone.

The *Wall Street Journal* in a study of 60 large U.S. companies found that they deposited $166 billion in offshore accounts in 2012, sheltering over 40% of their profits from U.S. taxes. Similarly, Desai, Foley and Hines in the *Journal of Public Economics* found that: "in 1999, 59% of U.S. firms with significant foreign operations had affiliates in tax haven countries", although they did not define "significant" for this purpose. In 2009, the U.S. Government Accountability Office (GAO) reported that 83 of the 100 largest U.S. publicly traded corporations and 63 of the 100 largest contractors for the U.S. federal government were maintaining subsidiaries in countries generally considered havens for avoiding taxes. The GAO did not review the companies' transactions to independently verify that the subsidiaries helped the companies reduce their tax burden, but said only that historically the purpose of such subsidiaries is to cut tax costs.

James Henry, former chief economist at consultants McKinsey & Company, in his report for the Tax Justice Network gives an indication of the amount of money that is sheltered by wealthy individuals in tax havens. The report estimated conservatively that a fortune of $21 trillion is stashed away in off-shore accounts with $9.8 trillion alone by the top tier—less than 100,000 people—who each own financial assets of $30 million or more. The report's author indicated that this hidden money results in a "huge" lost tax revenue—a "black hole" in the economy—and many countries would become creditors instead of being debtors if the money of their tax evaders would be taxed.

The Tax Justice Network estimated that global tax revenue lost in 2012 to tax havens is between US$190 billion and $255 billion per year, assuming a 3% capital gains rate, a 30% capital gains tax rate, and $21 trillion to $32 trillion hidden in tax havens worldwide. The Zucman study uses different methodology, and estimates lost

global tax revenue at US$190 billion. If such hidden offshore assets are considered, many countries with governments nominally in debt are shown to be net creditor nations.

The UN Economic Commission for Africa estimates that illegal financial flows cost the continent around $50 billion per year. The OECD estimates that two-thirds ($30 billion) occurs from tax avoidance and evasion from non-African firms. The continual avoidance of taxation by international corporations through legal and illegal methods stifles development in countries that greatly need such revenues to operate. The Sustainable Development Goals (SDGs) will be difficult to obtain if these loss of revenues continue to persist. Africa needs millions, if not billions, of dollars in order to meet the SDG's by 2030, which cannot simply come from foreign aid organizations.

In 2016 a massive data leak known as the "Panama Papers" cast some doubt on the size of previous estimates of lost revenue.

However, the tax policy director of the Chartered Institute of Taxation expressed skepticism over the accuracy of the figures. If true, those sums would amount to approximately 5 to 8 times the total amount of currency presently in circulation in the world. Daniel J. Mitchell of the Cato Institute says that the report also assumes, when considering notional lost tax revenue, that 100% money deposited offshore is evading payment of tax.

In October 2009, research commissioned from Deloitte for the Foot Review of British Offshore Financial Centres said that much less tax had been lost to tax havens than previously had been thought. The report indicated "We estimate the total UK corporation tax potentially lost to avoidance activities to be up to £2 billion per annum, although it could be much lower." An earlier report by the U.K. Trades Union Congress, concluded that tax avoidance by the 50 largest companies in the FTSE 100 was depriving the UK Treasury of approximately £11.8 billion. The report also stressed that British Crown Dependencies make a "significant contribution to the liquidity of the UK market". In the second quarter of 2009, they provided net funds to banks in the UK totaling $323 billion (£195 billion), of which $218 billion came from Jersey, $74 billion from Guernsey and $40 billion from the Isle of Man.

The Tax Justice Network reports that this system is "basically designed and operated" by a group of highly paid specialists from the world’s largest private banks (led by UBS, Credit Suisse, and Goldman Sachs), law offices, and accounting firms and tolerated by international organizations such as Bank for International Settlements, the International Monetary Fund, the World Bank, the OECD, and the G20. The

amount of money hidden away has significantly increased since 2005, sharpening the divide between the super-rich and the rest of the world.

Examples

The U.S. National Bureau of Economic Research has suggested that roughly 15% of the countries in the world are tax havens, that these countries tend to be small and affluent, and that better governed and regulated countries are more likely to become tax havens, and are more likely to be successful if they become tax havens.

- Switzerland
- Luxembourg – primarily a conduit tax haven

Other sovereign countries that have such low tax rates and lax regulation that they can be considered semi-tax havens are:

- Netherlands – primarily a conduit tax haven. *See also Dutch Sandwich*. Also, the Netherlands does not have a direct tax on royalties.
- Ireland. *See also double Irish (to cease by 2020) which is replaced by single malt* and also Irish Section 110 spv
- United States – favoured for its tax secrecy

Sub-national jurisdictions commonly labelled as tax havens include:

- Jersey (United Kingdom)
- Isle of Man (United Kingdom)
- British Overseas Territories
    - Bermuda
    - British Virgin Islands
    - Cayman Islands
- Delaware (United States)
- Puerto Rico (United States)

Some tax havens, including some of the ones listed above, do charge income tax as well as other taxes such as capital gains tax, inheritance tax, and so forth. Criteria distinguishing a taxpayer from a non-taxpayer can include citizenship and residency and source of income. For example, in the United States foreign nonresidents are not charged various taxes including income tax on interest on U.S. bank deposits by income tax; since the Clinton administration the IRS has proposed collecting

information on these depositors to share with their home countries as a regulation; these regulations were eventually finalized in April 2012.

In September 2013, British Prime Minister David Cameron said "I do not think it is fair any longer to refer to any of the Overseas Territories or Crown Dependencies as tax havens. They have taken action to make sure that they have fair and open tax systems. It is very important that our focus should now shift to those territories and countries that really are tax havens." Mr Cameron's comments were interpreted as a direct reference to Jersey, Guernsey, Isle of Man, the British Virgin Islands and the Cayman Islands, and followed a period of negotiations with those (and other) British territories during which those jurisdictions had made a number of concessions relating to tax transparency and sharing of information.

Former tax havens

- Beirut, Lebanon formerly had a reputation as the only tax haven in the Middle East. However, this changed after the Intra Bank crash of 1966, and the subsequent political and military deterioration of Lebanon dissuaded foreign use of the country as a tax haven.
- Liberia had a prosperous ship registration industry. The series of violent and bloody civil wars in the 1990s and early 2000s severely damaged confidence in the jurisdiction. The fact that the ship registration business still continues is partly a testament to its early success, and partly a testament to moving the national shipping registry to New York, United States.
- Tangier had a brief but colorful existence as a tax haven in the period between the end of effective control by the Spanish in 1945 until it was formally reunited with Morocco in 1956.
- A number of Pacific based tax havens have reduced their effectiveness to operate as tax havens in response to OECD demands for better regulation and transparency in the late 1990s. Vanuatu's Financial Services commissioner announced in May 2008 that his country would reform its laws so as to cease being a tax haven. "We've been associated with this stigma for a long time and we now aim to get away from being a tax haven."
- As of March 2013, major Cyprus banks have sustained severe damage from Greek bond defaults and (at least temporarily) closed their doors in an attempt to stem a flight of capital from the island. Depositors are expected to incur heavy losses.

The way tax havens operate can be viewed in the following principal contexts:

Personal residency

Since the early 20th century, wealthy individuals from high-tax jurisdictions have sought to relocate themselves in low-tax jurisdictions. In most countries in the world, residence is the primary basis of taxation. The low-tax jurisdictions chosen may levy no, or only very low, income tax and may not levy capital gains tax, or inheritance tax. Individuals are normally unable to return to their previous higher-tax country for more than a few days a year without reverting their tax residence to their former country. They are sometimes referred to as tax exiles.

Corporate residency

Corporate persons, in contrast to *natural persons*, are generally locked into their historic country, new corporations however can be established in a country of choice. Each corporation can establish subsidiary corporations in many countries, some for trading purposes and some with tax planning justification. That allows them to take advantage of the variety of laws, regulations, tax treaties and conventions in multiple countries, without overtly engaging in any questionable activities. Only in extreme cases will they move their formal corporate headquarters. The country of residency may choose what laws to pass to tax profits of their corporations and the profits of corporations resident elsewhere who trade in their country.

Asset holding

Asset holding involves utilizing an offshore trust or offshore company, or a trust owning a company. The company or trust will be formed in one tax haven, and will usually be administered and resident in another. The function is to hold assets, which may consist of a portfolio of investments under management, trading companies or groups, physical assets such as real estate or valuable chattels. The essence of such arrangements is that by changing the ownership of the assets into an entity which is not tax resident in the high-tax jurisdiction, they cease to be taxable in that jurisdiction.

Often the mechanism is employed to avoid a specific tax. For example, a wealthy testator could transfer his house into an offshore company; he can then settle the shares of the company on trust (with himself being a trustee with another trustee, whilst holding the beneficial life estate) for himself for life, and then to his daughter. On his death, the shares will automatically vest in the daughter, who thereby acquires the house, without the house having to go through probate and being assessed with inheritance tax. Most countries assess inheritance tax, and all other taxes, on real estate within their jurisdiction, regardless of the nationality of the owner, so this

would not work with a house in most countries. It is more likely to be done with intangible assets.

Trading and other business activity

Many businesses which do not require a specific geographical location or extensive labor are set up in a jurisdiction to minimize tax exposure. Perhaps the best illustration of this is the number of reinsurancecompanies which have migrated to Bermuda over the years. Other examples include internet based services and group finance companies. In the 1970s and 1980s corporate groups were known to form offshore entities for the purposes of "reinvoicing". These reinvoicing companies simply made a margin without performing any economic function, but as the margin arose in a tax free jurisdiction, it allowed the group to "skim" profits from the high-tax jurisdiction. Most sophisticated tax codes now prevent transfer pricing schemes of this nature.

Financial intermediaries

Much of the economic activity in tax havens today consists of professional financial services such as mutual funds, banking, life insurance and pensions. Generally the funds are deposited with the intermediary in the low-tax jurisdiction, and the intermediary then on-lends or invests the money (often back into a high-tax jurisdiction). Although such systems do not normally avoid tax in the principal customer's jurisdiction, it enables financial service providers to provide multi-jurisdictional products without adding another layer of taxation. This has proved particularly successful in the area of offshore funds.It has been estimated over 75% of the world's hedge funds, probably the riskiest form of collective investment vehicle, are domiciled in the Cayman Islands, with nearly $1.1 trillion US Assets under management although statistics in the hedge fund industry are notoriously speculative.

Anonymity and bearer shares

Bearer shares allow for anonymous ownership, and thus have been criticized for facilitating money laundering and tax evasion; these shares are also available in some OECD countries as well as in the U.S. state of Wyoming. In a 2010 study in which the researcher attempted to set-up anonymous corporations found that 13 of the 17 attempts were successful in OECD countries, such as the United States and the United Kingdom, while only 4 of 28 attempts were successful in countries typically labeled tax havens. The last two states in America permitting bearer shares, Nevada and Delaware made them illegal in 2007. In 2011, an OECD peer review recommended that the United Kingdom improve its bearer share laws. The UK abolished the use of bearer shares in 2015.

In 2012 the Guardian wrote that there are 28 persons as directors for 21,500 companies.

Money and exchange control

Most tax havens have a double monetary control system, which distinguish residents from non-resident as well as foreign currency from the domestic, the local currency one. In general, residents are subject to monetary controls, but not non-residents. A company, belonging to a non-resident, when trading overseas is seen as non-resident in terms of exchange control. It is possible for a foreigner to create a company in a tax haven to trade internationally; the company's operations will not be subject to exchange controls as long as it uses foreign currency to trade outside the tax haven. Tax havens usually have currency easily convertible or linked to an easily convertible currency. Most are convertible to US dollars, euro or to pounds sterling.

Incentives and benefits for tax haven countries

There are several reasons for a nation to become a tax haven. Some nations may find they do not need to charge as much as some industrialized countries in order for them to be earning sufficient income for their annual budgets. Some may offer a lower tax rate to larger corporations, in exchange for the companies locating a division of their parent company in the host country and employing some of the local population. Other domiciles find that this is a way to encourage conglomerates from industrialized nations to transfer needed skills to the local population.

According to Investopedia,

Although most offshore financial centers impose no corporate income tax, their governments still financially benefit from having thousands of companies registered in their jurisdiction. That is because tax haven governments typically impose a registration fee on all newly incorporated business entities like companies and partnerships. Also, companies are required to pay a renewal fee each year to still be recognized as an operating company.

There are also additional fees that are imposed on the companies depending on the type of business activity that they engage in. For example, banks, mutual funds and other companies in the financial services business usually need to pay for an annual license to operate in that industry. All of these various fees add up to create a strong source of recurring revenue for tax haven governments. It is estimated that the British Virgin Islands collects over $200 million each year in the form of corporate fees.

Many industrialized countries claim that tax havens act unfairly by reducing tax revenue which would otherwise be theirs. Various pressure groups also claim that money launderers also use tax havens extensively, although extensive financial and know your customer regulations in tax havens can actually make money laundering more difficult than in large onshore financial centers with significantly higher volumes of transactions, such as New York City or London. In 2000, the Financial Action Task Force published what came to be known as the "FATF Blacklist" of countries which were perceived to be uncooperative in relation to money laundering; although several tax havens have appeared on the list from time to time (including key jurisdictions such as the Cayman Islands, Bahamas and Liechtenstein), no offshore jurisdictions appear on the list at this time.

Regulation measures

To avoid tax competition, many high tax jurisdictions have enacted legislation to counter the tax sheltering potential of tax havens. Generally, such legislation tends to operate in one of five ways:

1. Attributing the income and gains of the company or trust in the tax haven to a taxpayer in the high-tax jurisdiction on an arising basis. Controlled Foreign Corporation legislation is an example of this.
2. Transfer pricing rules, standardization of which has been greatly helped by the promulgation of OECD guidelines.
3. Restrictions on deductibility, or imposition of a withholding tax when payments are made to offshore recipients.
4. Taxation of receipts from the entity in the tax haven, sometimes enhanced by notional interest to reflect the element of deferred payment. The EU withholding tax is probably the best example of this.
5. Exit charges, or taxing of unrealized capital gains when an individual, trust or company emigrates.

However, many jurisdictions employ blunter rules. For example, in France securities regulations are such that it is not possible to have a public bond issue through a company incorporated in a tax haven.

Also becoming increasingly popular is "forced disclosure" of tax mitigation schemes. Broadly, these involve the revenue authorities compelling tax advisors to reveal details of the scheme, so that the loopholes can be closed during the following tax year, usually by one of the five methods indicated above. Although not specifically aimed at tax havens, given that so many tax mitigation schemes involve the use of offshore structures, the effect is much the same.

Anti-avoidance came to prominence in 2010/2011 as nongovernmental organizations and politicians in the leading economies looked for ways of reducing tax avoidance, which plays a role in forcing unpopular cuts to social and military programs The International Financial Centres Forum (IFC Forum), a trade organisation for companies located in the British Overseas Territories and Crown Dependencies, has asked for a balanced debate on the issue of tax avoidance and an understanding of the role that the tax neutrality of small international financial centres plays in the global economy.

Modern developments

U.S. Legislation

The Foreign Account Tax Compliance Act (FATCA) was passed by the US Congress to stop the outflow of money from the country into tax haven bank accounts. With the strong backing of the Obama Administration, Congress drafted the FATCA legislation and added it into the Hiring Incentives to Restore Employment Act (HIRE) signed into law by President Obama in March 2010.

FATCA requires foreign financial institutions (FFI) of broad scope – banks, stock brokers, hedge funds, pension funds, insurance companies, trusts – to report directly to the Internal Revenue Service (IRS) all clients who are U.S. persons. Starting January 2014, FATCA requires FFIs to provide annual reports to the IRS on the name and address of each U.S. client, as well as the largest account balance in the year and total debits and credits of any account owned by a U.S. person. If an institution does not comply, the U.S. will impose a 30% withholding tax on all its transactions concerning U.S. securities, including the proceeds of sale of securities.

In addition, FATCA requires any foreign company not listed on a stock exchange or any foreign partnership which has 10% U.S. ownership to report to the IRS the names and tax identification number (TIN) of any U.S. owner. FATCA also requires U.S. citizens and green card holders who have foreign financial assets in excess of $50,000 to complete a new Form 8938 to be filed with the 1040 tax return, starting with fiscal year 2010. The delay is indicative of a controversy over the feasibility of implementing the legislation as evidenced in this paper from the Peterson Institute for International Economics.

An unintended consequence of FATCA and its cost of compliance for non-US banks is that some non-US banks are refusing to serve American investors. Concerns have also been expressed that, because FATCA operates by imposing withholding taxes on U.S. investments, this will drive foreign financial institutions (particularly hedge

funds) away from investing in the U.S. and thereby reduce liquidity and capital inflows into the US.

Tax Justice Network Report 2012

A 2012 report by the British Tax Justice Network estimated that between US$21 trillion and $32 trillion is sheltered from taxes in unreported tax havens worldwide. If such wealth earns 3% annually and such capital gains were taxed at 30%, it would generate between $190 billion and $280 billion in tax revenues, more than any other tax shelter. If such hidden offshore assets are considered, many countries with governments nominally in debt are shown to be net creditor nations. However, despite being widely quoted, the methodology used in the calculations has been questioned, and the tax policy director of the Chartered Institute of Taxation also expressed skepticism over the accuracy of the figures. Another recent study estimated the amount of global offshore wealth at the smaller—but still sizable—figure of US$7.6 trillion. This estimate included financial assets only: "My method probably delivers a lower bound, in part because it only captures financial wealth and disregards real assets. After all, high-net-worth individuals can stash works of art, jewelry, and gold in 'freeports,' warehouses that serve as repositories for valuables—Geneva, Luxembourg, and Singapore all have them. High-net-worth individuals also own real estate in foreign countries." A study of 60 large US companies found that they deposited $166 billion in offshore accounts during 2012, sheltering over 40% of their profits from U.S. taxes.

Bank data leak 2013

Details of thousands of owners of offshore companies were published in April 2013 in a joint collaboration between *The Guardian* and the International Consortium of Investigative Journalists. The data was later published on a publicly accessible website in an attempt to "crowd-source" the data. The publication of the list appeared to be timed to coincide with the 2013 G8 summit chaired by British Prime Minister David Cameron which emphasised tax evasion and transparency.

Liechtenstein banking scandal

Germany announced in February 2008 that it had paid €4.2 million to Heinrich Kieber a former data archivist of LGT Treuhand, a Liechtenstein bank, for a list of 1,250 customers of the bank and their accounts' details. Investigations and arrests followed relating to charges of illegal tax evasion. The German authorities shared the data with U.S. tax authorities, but the British government paid a further £100,000 for the same data. Other governments, notably Denmark and Sweden, refused to pay for

the information regarding it as stolen property. The Liechtenstein authorities subsequently accused the German authorities of espionage.

However, regardless of whether unlawful tax evasion was being engaged in, the incident has fuelled the perception among European governments and the press that tax havens provide facilities shrouded in secrecy designed to facilitate unlawful tax evasion, rather than legitimate tax planning and legal tax mitigation schemes. This in turn has led to a call for "crackdowns" on tax havens. Whether the calls for such a crackdown are mere posturing or lead to more definitive activity by mainstream economies to restrict access to tax havens is yet to be seen. No definitive announcements or proposals have yet been made by the European Union or governments of the member states.

German legislation

Peer Steinbrück, the former German finance minister, announced in January 2009 a plan to amend fiscal laws. New regulations would disallow that payments to companies in certain countries that shield money from disclosure rules to be declared as operational expenses. The effect of this would make banking in such states unattractive and expensive.

UK Foot report

In November 2009, Sir Michael Foot, a former Bank of England official and Bahamas bank inspector, delivered a report on the British Crown Dependencies and Overseas Territories for HM Treasury. The report indicated that while many of the territories "had a good story to tell", others needed to improve their abilities to detect and prevent financial crime. The report also stressed the view that narrow tax bases presented long term strategic risks and that the economies should seek to diversify and broaden their tax bases.

It indicated that tax revenue lost by the UK government appeared to be much smaller than had previously been estimated , and also stressed the importance of the liquidity provided by the territories to the United Kingdom. The Crown Dependencies and Overseas Territories broadly welcomed the report. The pressure group Tax Justice Network, unhappy with the findings, commented that "[a] weak man, born to be an apologist, has delivered a weak report."

G20 tax haven blacklist

At the London G20 summit on 2 April 2009, G20 countries agreed to define a blacklist for tax havens, to be segmented according to a four-tier system, based on

compliance with an "internationally agreed tax standard." The list as per 2 April 2009 can be viewed on the OECD website. The four tiers were:

1. Those that have substantially implemented the standard (includes most countries but China still excludes Hong Kong and Macau).
2. Tax havens that have committed to – but not yet fully implemented – the standard (includes Montserrat, Nauru, Niue, Panama, and Vanuatu)
3. Financial centres that have committed to – but not yet fully implemented – the standard (includes Guatemala, Costa Rica and Uruguay).
4. Those that have not committed to the standard (an empty category)

Those countries in the bottom tier were initially classified as being 'non-cooperative tax havens'. Uruguay was initially classified as being uncooperative. However, upon appeal the OECD stated that it did meet tax transparency rules and thus moved it up. The Philippines took steps to remove itself from the blacklist and Malaysian Prime Minister Najib Razak had suggested earlier that Malaysia should not be in the bottom tier.

In April 2009 the OECD announced through its chief Angel Gurria that Costa Rica, Malaysia, the Philippines and Uruguay have been removed from the blacklist after they had made "a full commitment to exchange information to the OECD standards." Despite calls from the former French President Nicolas Sarkozy for Hong Kong and Macau to be included on the list separately from China, they are as yet not included independently, although it is expected that they will be added at a later date.

Government response to the crackdown has been broadly supportive, although not universal. Luxembourg Prime Minister Jean-Claude Juncker has criticised the list, stating that it has "no credibility", for failing to include various states of the USA which provide incorporation infrastructure which are indistinguishable from the aspects of pure tax havens to which the G20 object. As of 2012, 89 countries have implemented reforms sufficient to be listed on the OECD's white list. According to Transparency International half of the least corrupted countries were tax havens.

EU tax haven blacklist

In December 2017, European Union adopted blacklist of tax havens in a bid to discourage the most aggressive tax dodging practices. It also had a so-called gray list which includes those who have committed to change their rules on tax transparency and cooperation. The 17 blacklisted territories are: American Samoa, Bahrain, Barbados, Grenada, Guam, South Korea, Macau, The Marshall Islands, Mongolia, Namibia, Palau, Panama, Saint Lucia, Samoa, Trinidad and Tobago, Tunisia, United Arab Emirates. Some activists denounced the listing process

as a whitewash and had called for the inclusion in the blacklist of some EU countries accused of facilitating tax avoidance, like Luxembourg, Malta, Ireland and the Netherlands.

Criticism

Tax havens have been criticized because they often result in the accumulation of idle cashwhich is expensive and inefficient for companies to repatriate. The tax shelter benefits result in a tax incidence disadvantaging the poor outside the tax haven. Many tax havens are thought to have connections to fraud, money laundering and terrorism. While investigations of illegal tax haven abuse have been ongoing, there have been few convictions. Lobbying pertaining to tax havens and associated transfer pricing has also been criticized.

Some politicians, such as magistrate Eva Joly, have begun to stand up against the use of tax havens by large companies. She describes the act of avoiding tax as a threat to democracy. Accountants' opinions on the propriety of tax havens have been evolving, as have the opinions of their corporate users, governments, and politicians, although their use by Fortune 500companiesand others remains widespread. Reform proposals centering on the Big Four accountancy firms have been advanced. Some governments appear to be using computer spyware to scrutinize some corporations' finances.

Effect of developing countries

Illicit capital flight from the developing world is estimated at ten times the size of aid it receives and twice the debt service it pays. About 60 per cent of illicit capital flight from Africa is from transfer mispricing, where a subsidiary in a developing nation sells to another subsidiary or shell company in a tax haven at an artificially low price to pay less tax. An African Union report estimates that about 30% of sub-Saharan Africa's GDP has been moved to tax havens. One tax analyst believes that if the money were paid, most of the continent would be "developed" by now.

History

The use of differing tax laws between two or more countries to try to mitigate tax liability is probably as old as taxation itself. In Ancient Greece, some of the Greek Islands were used as depositories by the sea traders of the era to place their foreign goods to thus avoid the two-percent tax imposed by the city-state of Athens on imported goods. The practice may have first reached prominence through the avoidance of the Cinque Ports and later the staple ports in the twelfth and fourteenth

centuries respectively. In 1721, American colonies traded from Latin America to avoid Britishtaxes.

Various countries claim to be the oldest tax haven in the world. For example, the Channel Islands claim their tax independence dating as far back as Norman Conquest, while the Isle of Man claims to trace its fiscal independence to even earlier times. Nonetheless, the modern concept of a tax haven is generally accepted to have emerged at an uncertain point in the immediate aftermath of World War I. Bermudasometimes optimistically claims to have been the first tax haven based upon the creation of the first offshore companies legislation in 1935 by the newly created law firm of Conyers Dill & Pearman. However, the Bermudian claim is debatable when compared against the enactment of a Trust Law by Liechtenstein in 1926 to attract offshore capital.

Most economic commentators suggest that the first "true" tax haven was Switzerland, followed closely by LiechtensteinSwiss banks had long been a *capital haven* for people fleeing social upheaval in Russia, Germany, South America and elsewhere. However, in the early part of the twentieth century, during the years immediately following World War I, many European governments raised taxes sharply to help pay for reconstruction efforts following the devastation of World War I. By and large, Switzerland, having remained neutral during the Great War, avoided these additional infrastructure costs and was consequently able to maintain a low level of taxes. As a result, there was a considerable influx of capital into the country for tax related reasons. It is difficult, nonetheless, to pinpoint a single event or precise date which clearly identifies the emergence of the modern tax haven.

The use of modern tax havens has gone through several phases of development subsequent to the interwar period. From the 1920s to the 1950s, tax havens were usually referenced as the avoidance of personal taxation. The terminology was often used with reference to countries to which a person could retire and mitigate their post retirement tax position, a usage which was still being echoed to some degree in a 1990 report, which included indications of quality of life in various tax havens which future tax exiles may wish to consider.

From the 1950s onward, there was significant growth in the use of tax havens by corporate groups to mitigate their global tax burden. The strategy generally relied upon there being a double taxation treatybetween a large jurisdiction with a high tax burden (that the company would otherwise be subject to), and a smaller jurisdiction with a low tax burden. By structuring the group ownership through the smaller jurisdiction, corporations could take advantage of the double taxation treaty, paying taxes at the much lower rate. Although some of these double tax treaties survive for example between Barbados and Japan,

between Cyprus and Russia and Mauritius with India, which India sought to renegotiate in 2007, most major countries began repealing their double taxation treaties with micro-states in the 1970s, to prevent corporate tax leakage in this manner.

In the early to mid-1980s, most tax havens changed the focus of their legislation to create corporate vehicles which were "ring-fenced" and exempt from local taxation (although they usually could not trade locally either). These vehicles were usually called "exempt companies" or "international business corporations". However, in the late 1990s and early 2000s, the OECD began a series of initiatives aimed at tax havens to curb the abuse of what the OECD referred to as "unfair tax competition". Under pressure from the OECD, most major tax havens repealed their laws permitting these ring-fenced vehicles to be incorporated, but concurrently they amended their tax laws so that a company which did not actually trade within the jurisdiction would not accrue any local tax liability.

Terrorism financing

Terrorism financing refers to activities that provides financing or financial support to individual terrorists or terrorist groups . A government that maintains a list of terrorist organizations normally will also pass laws to prevent money laundering being used to finance those organizations.

Laws against money laundering and terror financing are used around the world. In the United States, the Patriot Act was passed after the September 11 attacks, giving the government anti-money laundering powers to monitor financial institutions. The Patriot Act has generated a great deal of controversy in the United States since its enactment. The United States has also collaborated with the United Nations and other countries to create the Terrorist Finance Tracking Program.

Laws created attempted to thwart the financing of terrorism (CFT) and money laundering. Initially the focus of CFT efforts was on non-profit organizations, unregistered money services businesses (MSBs) (including so called underground banking or 'Hawalas') and the criminalisation of the act itself. The Financial Action Task Force on Money Laundering (FATF) made nine special recommendations for CFT (first eight then a year later added a ninth). These nine recommendations have become the global standard for CFT and their effectiveness is assessed almost always in conjunction with anti-money laundering.

The FATF Blacklist (the NCCT list) mechanism was used to coerce countries to bring about change.

Money laundering

Often linked in legislation and regulation, terrorism financing and money laundering are conceptual opposites. Money laundering is the process where cash raised from criminal activities is made to look legitimate for re-integration into the financial system, whereas terrorism financing cares little about the source of the funds, but it is what the funds are to be used for that defines its scope.

An in-depth study of the symbiotic relationship between organised crime and terrorist organizations detected within the United States of America and other areas of the world referred to as crime-terror nexus points has been published in the forensic literature. The Perri, Lichtenwald and MacKenzie article emphasizes the importance of multi-agency working groups and the tools that can be used to identify, infiltrate, and dismantle organizations operating along the crime-terror nexus points.

Terrorists use low value but high volume fraud activity to fund their operations. Paramilitary groups in Northern Ireland are usinglegitimate businesses such as hotels, pubs and taxi operators to launder money and fund political activities. Even beyond Ireland, terrorists are buying out/controlling front-end businesses especially cash-intensive businesses including in some cases money services businesses to move monies. Bulk cash smuggling and placement through cash-intensive businesses is one typology. They are now also moving monies through the new online payment systems. They also use trade linked schemes to launder monies. Nonetheless, the older systems have not given way. Terrorists also continue to move monies through MSBs/Hawalas, and through international ATM transactions. Charities also continue to be used in countries where controls are not so stringent.

Suspicious activity

Operation Green Quest, a US multi-agency task force established in October 2001 with the official purpose of countering terrorism financing considers the following patterns of activity as indicators of the collection and movement of funds that could be associated with terrorism financing:

- Account transactions that are inconsistent with past deposits or withdrawals such as cash, cheques, wire transfers, etc.
- Transactions involving a high volume of incoming or outgoing wire transfers, with no logical or apparent purpose that come from, go to, or transit through locations of concern, that is sanctioned countries, non-cooperative nations and sympathizer nations.
- Unexplainable clearing or negotiation of third party cheques and their deposits in foreign bank accounts.
- Structuring at multiple branches or the same branch with multiple activities.
- Corporate layering, transfers between bank accounts of related entities or charities for no apparent reasons.
- Wire transfers by charitable organisations to companies located in countries known to be bank or tax havens.
- Lack of apparent fund raising activity, for example a lack of small cheques or typical donations associated with charitable bank deposits.
- Using multiple accounts to collect funds that are then transferred to the same foreign beneficiaries
- Transactions with no logical economic purpose, that is, no link between the activity of the organization and other parties involved in the transaction.
- Overlapping corporate officers, bank signatories, or other identifiable similarities associated with addresses, references and financial activities.

- Cash debiting schemes in which deposits in the US correlate directly with ATM withdrawals in countries of concern. Reverse transactions of this nature are also suspicious.
- Issuing cheques, money orders or other financial instruments, often numbered sequentially, to the same person or business, or to a person or business whose name is spelled similarly.

It would be difficult to determine by such activity alone whether the particular act was related to terrorism or to organized crime. For this reason, these activities must be examined in context with other factors in order to determine a terrorism financing connection. Simple transactions can be found to be suspect and money laundering derived from terrorism will typically involve instances in which simple operations had been performed (retail foreign exchange operations, international transfer of funds) revealing links with other countries including FATF blacklisted countries. Some of the customers may have police records, particularly for trafficking in narcotics and weapons and may be linked with foreign terrorist groups. The funds may have moved through a state sponsor of terrorism or a country where there is a terrorism problem. A link with a Politically exposed person (PEP) may ultimately link up to a terrorism financing transaction. A charity may be a link in the transaction. Accounts (especially student) that only receive periodic deposits withdrawn via ATM over two months and are dormant at other periods could indicate that they are becoming active to prepare for an attack.

Germany

In July 2010, Germany outlawed the Internationale Humanitäre Hilfsorganisation (IHH), saying it has used donations to support projects in Gaza that are related to Hamas, which is considered by the European Union to be a terrorist organization, while presenting their activities to donors as humanitarian help. German Interior Minister Thomas de Maiziere said, "Donations to so-called social welfare groups belonging to Hamas, such as the millions given by IHH, actually support the terror organization Hamas as a whole."

Australia

In 2009, an investigation carried out by the Australian Transaction Reports and Analysis Centre (AUSTRAC) and other agencies, determined that funds were being sent from Australia for use by the Somalia-based terrorist group, al-Shabaab. Money was remitted, with false names used to obscure the money trail. This investigation lead to the ultimate arrest of the suspects on charges of conspiring to commit a terrorist attack on an Australian army base.

In 2014, Australian authorities feared that money being transferred from Australia could be used for terrorism in Somalia. In 2015 Australian banks ceased providing money-transfer facilities to Somalia.

Terrorist Finance Tracking Program

The **Terrorist Finance Tracking Program** (**TFTP**) is a United States government program to access financial transactions on the international SWIFT network that was revealed by *The New York Times*, *The Wall Street Journal* and *The Los Angeles Times* in June 2006. It was part of the Bush administration's War on Terrorism. After the covert action was disclosed, the so-called SWIFT Agreement was negotiated between the United States and the European Union.

A series of articles published on June 23, 2006, by the *New York Times*, the *Wall Street Journal* and the *Los Angeles Times* revealed that the United States government, specifically the Treasury and the CIA, had a program to access the SWIFT transaction database after the September 11th attacks.

According to the June 2006 *New York Times* article, the program helped lead to the capture of an al-Qaeda operative known as Hambali in 2003, believed to be the mastermind of the 2002 Bali bombing, as well as helped identify a Brooklyn man convicted in 2005 for laundering money for an al-Qaeda operative in Pakistan. The Treasury Department and White House responded to the leak the day before it was published, and claimed that the leak damaged counterterrorism activities. They also referred to the program as the "Terrorist Finance Tracking Program" ("TFTP"), similar to the Terrorist Surveillance Program in the NSA wiretapping controversy.

The Terrorist Finance Tracking Program was viewed by the Bush administration as another tool in the "Global War on Terrorism". The administration contends the program allows additional scrutiny that could prove instrumental in tracking transactions between terrorist cells. Some have raised concerns that this classified program might also be a violation of United States and European financial privacy laws, because individual search warrants to access financial data were not obtained in advance. In response to the claim that the program violates U.S. law, some have noted that the U.S. Supreme Court in *United States v. Miller* (1976) has ruled that there is not an expected right to privacy for financial transaction records held by third parties and that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed".

Immediately following the disclosure, SWIFT released an official press statement asserting that they did give information to the United States in compliance with

Treasury Department subpoenas, but claiming that "SWIFT received significant protections and assurances as to the purpose, confidentiality, oversight and control of the limited sets of data produced under the subpoenas".

On 27 June 2006, it was revealed by the media that Belgium's central bank, the National Bank of Belgium, had known about the U.S. government's access to the SWIFT databases since 2002. Belgian Christian Democratic and Flemish party claimed on June 28, that the actions of the CIA with SWIFT were in breach with Belgian privacy laws. The Belgian parliamentary committee that deals with the workings of the Belgian State Security Service (*Comité I*) reported that SWIFT was indeed in violation with Belgian and European privacy laws.

In addition, the New York branch of the Dutch Rabobank is said to deliver information on its European customers to the U.S. government, in contempt of European privacy laws. The Dutch Data Protection Authority claims that Dutch banks could face fines if they hand over data on their customers to the U.S. government.

Consequently, the European Union (EU) obtained an agreement that they could send an investigating magistrate as High Representative of the EU to the United States of America in order to monitor the TFTP activities. This magistrate, Jean-Louis Bruguière, had a permanent office in Washington, D.C., at the U.S. Department of Treasury.

Disclosures by former National Security Agency contractor Edward Snowden alleged the NSA was systematically undermining the SWIFT Agreement. No denial was issued by the American side, and the European Parliament passed a non-binding vote calling for the suspension the agreement. A suspension would however require the consent of a two-thirds majority of EU governments.

EU-U.S. relations

Legal treaty development

After European concerns with wholesale SWIFT data export were raised, it became necessary for the United States to negotiate a treaty with the EU in order to be able to continue accessing the SWIFT database. The *Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program* was negotiated during 2009. The treaty was first rejected by the European parliament, however after a few months and a visit by U.S. Vice president Joe Biden to the parliament, the European Commission introduced a proposal with strengthened safeguards, which was then adopted.

Scope

The scope of the treaty is to use financial payment messaging data to prevent, investigate, detect, and prosecute conduct pertaining to terrorism or terrorist financing. Terrorism is defined as acts which involves violence or are otherwise dangerous to human life or create a risk of damage to property or infrastructure with the intent to intimidate a population or government or an international institution to act or abstain from acting or to seriously destabilize or destroy fundamental structures of a country or international organization.

Process

The United States Treasury serves production orders to a designated provider of financial data. SWIFT is the only designated provider today. The request shall identify as clearly as possible the data necessary for the purpose of the treaty. The request should clearly substantiate the necessity of the data, and be tailored as narrowly as possible. Payments within the Single Euro Payments Area are excluded.

Safeguards

The U.S. Treasury shall process the data only for the purpose of the treaty and data mining is not allowed. The data must be secured and cannot be interconnected with any other database. Access to data shall be limited to investigations of terrorism. All searches must be based upon preexisting information or evidence of connection with terrorism. Information may only be shared with law enforcement, public security, or counterterrorism authorities in the United States or the EU.

Citizen's rights

Any person has the right to obtain a confirmation through the data protection authority in the EU member state that the person's data protection rights have been respected. Any person has the right to seek the rectification, erasure or blocking of his or her personal data where the data is inaccurate or the processing contravenes the treaty.

European TFTP

EU may request the aid of the United States to build up a European TFTP.

References

1. *Duhaime, Christine. "What is Laundering? Duhaime's Financial Crime and Anti-Money Laundering Law". Retrieved 7 March 2014.*
2. *"Financial Weapons of War, Minnesota Law Review (2016)". ssrn.com. SSRN 2765010.*
3. See for example the Anti-Money Laundering & Counter Terrorism Financing Act 2006 (Australia), the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (New Zealand), and the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap 615) (Hong Kong. See also (for example) guidance on IMF and FATF websites similarly conflating the concepts.
4. *"Anti-Money Laundering – Getting The Deal Through – GTDT". Getting The Deal Through. Retrieved 28 May 2017.*
5. *Sterling Seagrave (1995). Lord of the RIM.*
6. *Nigel Morris-Cotterill (1999). "A brief history of money laundering".*
7. *Protess, Ben & Jessica Silver-Greenberg (30 June 2014). "BNP Paribas Admits Guilt and Agrees to Pay $8.9 Billion Fine to U.S." The New York Times. Retrieved 1 July 2014.*
8. *"AUSTRAC at a glance". AUSTRAC. Retrieved 18 August 2016.*
9. *Reuter, Peter (2004). Chasing Dirty Money. Peterson. ISBN 978-0-88132-370-2.*
10. *"History of Anti-Money Laundering Laws". United States Department of the Treasury. 30 June 2015. Retrieved 30 June 2015.*
11. Lawrence M. Salinger, *Encyclopedia of white-collar & corporate crime: A – I, Volume 1*, page 78, ISBN 0-7619-3004-3, 2005.
12. *National Drug Intelligence Center (August 2011). "National Drug Threat Assessment" (PDF). p. 40. Retrieved 20 September 2011.*
13. *"National Money Laundering Threat Assessment" (PDF). December 2005. p. 33. Archived from the original (PDF) on 17 October 2010. Retrieved 3 March 2011.*
14. *Baker, Raymond (2005). Capitalism's Achilles Heel. Wiley.*
15. *Financial Action Task Force. "Global Money Laundering and Terrorist Financing Threat Assessment" (PDF). Retrieved 3 March 2011.*
16. http://www.private-eye.co.uk/registry
17. *"Underground Economy Issues. Ontario Construction Secretariat". Archived from the originalon 16 December 2010.*
18. *"Tax amnesties turn HMRC into 'biggest money-laundering operation in history'". Retrieved 14 June 2013.*
19. *"Money Laundering: the Importance of International Countermeasures--Address by Michel Camdessus". IMF. Retrieved 2018-03-02.*

20. *Financial Action Task Force. "Money Laundering FAQ". Retrieved 2 March 2011.*
21. For example, under UK law the first offences created for money laundering both related to the proceeds from the sale of illegal narcotics under the Criminal Justice Act 1988 and then later under the Drug Trafficking Act 1994.
22. *Richet, Jean-Loup (June 2013). "Laundering Money Online: a review of cybercriminals methods". arXiv:1310.2368* .
23. *Zetter, Kim (May 2013). "Liberty Reserve founder indicted on $6 billion money-laundering charges". Wired. Retrieved 20 October 2013.*
24. *Solon, Olivia (October 2013). "Cybercriminals launder money using in-game currencies". Wired. Retrieved 22 October 2013.*
25. *International Federation of Accountants. "Anti-Money Laundering" (PDF). Retrieved 27 March 2014.*
26. *Cassella, S.D. (2003). "Reverse money laundering". Journal of Money Laundering Control. **7**(1): 92–94.*
27. *Zabyelina, Yuliya (2015). "Reverse money laundering in Russia: Clean cash for dirty ends". Journal of Money Laundering Control. **18** (2): 202–21. doi:10.1108/JMLC-10-2014-0039.*
28. EAG (2012). "Money laundering and terrorist financing with use of physical cash and bearer instruments", 17th Plenary Meeting of the Eurasian Group on Combating Money Laundering and Financing of Terrorism, 28 December, New Delhi.
29. *Financial Action Task Force. "About the FATF". Retrieved 20 September 2011.*
30. *Financial Action Task Force. "About the Non-Cooperative Countries and Territories (NCCT) Initiative". Retrieved 20 September 2011.*
31. *"The Global Anti-Money Laundering Regime: A Short Overview, by Richard Horowitz, Cayman Islands Journal, 6 January 2010". Compasscayman.com. Retrieved 10 November2013.*
32. *Financial Action Task Force. "Money Laundering FAQ". Retrieved 20 September 2011.*
33. *"Financial Crime Job Descriptions - FinCrimeJobs.com".*
34. *Roth, John; et al. (20 August 2004). "Monograph on Terrorist Financing" (PDF). National Commission on Terrorist Attacks Upon the United States. pp. 54–56. Retrieved 20 September2011.*
35. *Ball, Deborah, et al., (22 March 2011). "U.S. Banks Oppose Tighter Money Rules". Wall Street Journal. Retrieved 19 September 2011.*
36. *Money Laundering Bulletin*, Issue 154, June 2008, Dr Jackie Harvey (Newcastle Business School
37. *"The Lost Trail". The Economist. 20 October 2005. Retrieved 19 September 2011.*

38. *Levi, Michael & William Gilmore (2002). "Terrorist Finance, Money Laundering and the Rise of Mutual Evaluation: A New Paradigm for Crime Control?". European Journal of Law Reform. **4** (2): 337–364.*
39. *Levi, Michael (May 2010). "Combating the Financing of Terrorism: A History and Assessment of the Control of 'Threat Finance'". The British Journal of Criminology. **50** (4): 650–669. doi:10.1093/bjc/azq025.*
40. *"Coming clean". The Economist. 14 October 2004. Archived from the original on 15 June 2013.*
41. *Bartlett, Brent (May 2002). "The Negative Effects of Money Laundering on Economic Development". Asian Development Bank. Archived from the original on 2 June 2011. Retrieved 19 September 2011.*
42. *Article 29 Data Protection Working Party. "Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing" (PDF). European Commission. Retrieved 18 February 2014.*
43. *Article 29 Data Protection Working Group. "Opinion 14/2011 Annex: Recommendations"(PDF). European Commission. Retrieved 18 February 2014.*
44. *American Civil Liberties Union. "The Surveillance Industrial Complex" (PDF). Retrieved 23 October 2011.*
45. *Mallen, Patricia (13 February 2013). "In Mexico, Around $10B Every Year Come From Money Laundering, Which Was Not Illegal in 16 Out of 31 States". International Business Times. Retrieved 12 March 2014.*
46. *GAFI, FATF (21 July 2017). "FATF Members and Observers". www.fatf-gafi.org.*
47. *Financial Action Task Force. "Member Country and Observers FAQ".*
48. *"Mission". Retrieved 21 June 2014.*
49. *"High-risk and non-cooperative jurisdictions". www.fatf-gafi.org. 23 June 2017.* |first1=missing |last1= in Authors list (help)
50. International Money Laundering Information Network. Retrieved on 21 October 2011.
51. World Bank Financial Market Integrity. Amlcft.org. Retrieved on 21 October 2011.
52. *"fintraca.gov.af". fintraca.gov.af. Retrieved 10 November 2013.*
53. Australian National Security: What Australia is doing
54. *Financial Transaction Reports Act 1988* (Cth), s 24.
55. *Tyree, Alan (1997). Digital Cash. Adelaide, Australia: Butterworths. pp. 82, 86. ISBN 0 409 31316 5.*
56. *"Money Laundering Act 2012 amended". Resource Portal of OGR Legal. OGR Legal. Retrieved 2 November 2015.*
57. *"Laws and Acts". Bangladesh Bank.*
58. *Duhaime, Christine. "AML Legislation in Canada, Duhaime's Financial Crime and Anti-Money Laundering Law". Retrieved 7 March 2014.*

59. *"AML global alignment: Two steps forward, one step back"* *(PDF)*. *pwc.com. PwC Financial Services Regulatory Practice, June 2015.*
60. *"EUR-Lex – 52013PC0045 – EN – EUR-Lex".*
61. *"Prevention of Money Laundering Act, 2002"* *(PDF)*. *Financial Intelligence Unit (FIU-IND), Ministry of Finance, India. Retrieved 10 October 2012.*
62. *"The Prevention of Money Laundering (Amendment) Act, 2005"* *(PDF)*. *Retrieved 10 November 2013.*
63. *"The Prevention of Money Laundering (Amendment) Act, 2009"* *(PDF)*. *Retrieved 10 November 2013.*